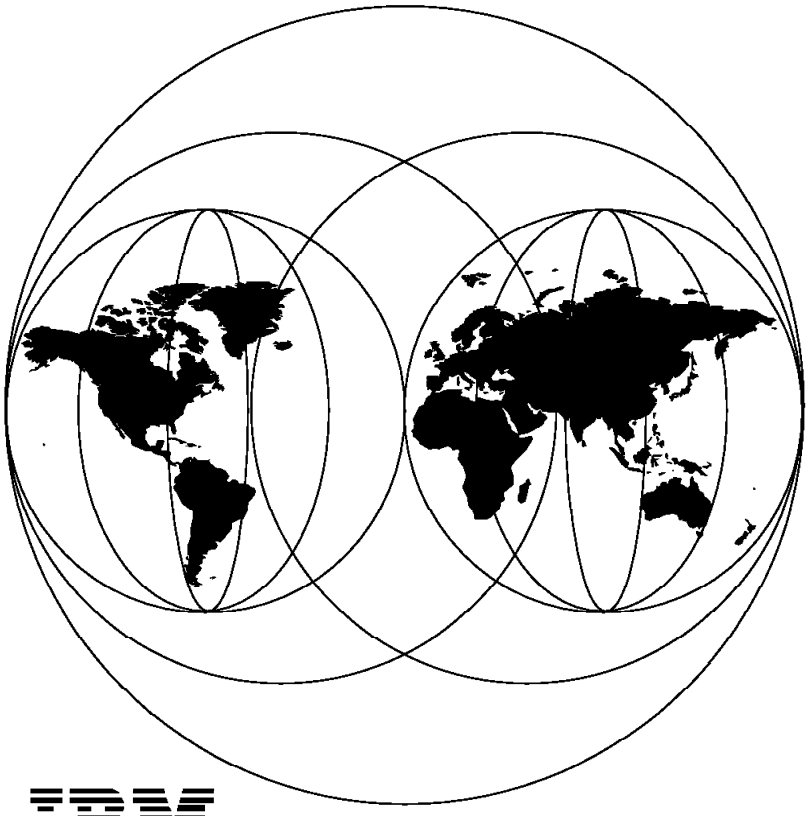
SG24-4692-00

Automating Problem Resolution with SystemView for OS/2

June 1996



IBM

International Technical Support Organization
Raleigh Center

International Technical Support Organization

SG24-4692-00

Automating Problem Resolution with SystemView for OS/2

June 1996

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix B, “Special Notices” on page 219.

First Edition (June 1996)

This edition applies to Version 1.0 of SystemView for OS/2, Program Number 5801-AAR for use with the OS/2 V3.0 Operating System.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Preface

This redbook provides detailed coverage of SystemView for OS/2 and its automation capabilities. It focuses on extending the product's usability and extending its integration with other products to provide systems management solutions. In addition, it provides examples of these solutions across many different operating systems.

This book was written for technical professionals who have some knowledge of systems management and automation.

How This Redbook Is Organized

The redbook is organized as follows:

- Chapter 1, "Overview of Automation Functions"

  This chapter provides an overview of the automation process as it relates to SystemView for OS/2.

- Chapter 2, "AntiVirus"

  This chapter provides details on how to integrate IBM AntiVirus with SystemView for OS/2. We show examples of how to take an automated action on multiple operating systems if a virus is detected.

- Chapter 3, "Automating ADSM/2 Using SystemView/2"

  This chapter show how to integrate the command line interface for ADSM/2 with SystemView for OS/2.

- Chapter 4, "Automating Software Package Install"

  This chapter show how to do some automated software distribution based upon alerts that flow to SystemView for OS/2.

- Chapter 5, "System Monitor"

  This chapter shows many of the monitors that come with SystemView for OS/2 and describes their functions.

- Chapter 6, "Serial Connections"

  This chapter show how to automate the connection of a remote LAN segment to SystemView for OS/2 using a serial connection.

- Chapter 7, "Creating Policies for New SystemView Clients"

  This chapter discusses SystemView for OS/2s INI files.

- Chapter 8, "Windows 95 Management"

  This chapter shows how to use the Windows 95 client.

- Chapter 9, "Problem Determination Data"

  This chapter shows how to automate the gathering of problem determination information to be fed to SystemView for OS/2.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the Systems Management and Networking ITSO Center, Raleigh.

Barry Nusbaum is a Senior ITSO Specialist for AIX, OS/2 and NT Systems Management at the Systems Management and Networking ITSO Center, Raleigh. He writes extensively and teaches IBM classes worldwide on all areas of OS/2, AIX and NT systems management. Before joining the ITSO 4 years ago, Barry D. Nusbaum worked in Professional Services in the US as the National Communications Specialist.

Leonardo Pires Frollini is a systems specialist in Brazil. He has several years of experience in systems management.

Hans-Juergen Lehn is a systems specialist in Germany. He has several years of experience in systems management.

Victor Torres is a systems specialist in Mexico. He has several years of experience in systems management.

Thanks to the following people for their invaluable contributions to this project:

Tim Kearby
Systems Management and Networking ITSO Center, Raleigh

Sam Thompsam and David Young
IBM RTP

Nina Insolia and Antonio Taurisano
IBM Rome

Comments Welcome

We want our redbooks to be as helpful as possible. Should you have any comments about this or other redbooks, please send us a note at the following address:

redbook@vnet.ibm.com

Your comments are important to us!

Chapter 1. Overview of Automation Functions

This chapter provides an overview of the automation features that are associated with SystemView for OS/2. The topics covered are:

- SystemView for OS/2 Alerts
- Components that issue alerts
- Genalerts
- Alert flows
- Action Editor
- Passing Alerts onto other operating systems

SystemView for OS/2 is the newest member of IBM′s SystemView series. It offers a comprehensive set of systems management functions to help users improve control and availability of their computer resources in a workgroup environment. It also helps them to pro-actively deal with problems and contain the costs associated with running and maintaining their Intel desktop machines and servers. This includes OS/2, Windows 3.1, Windows 95, Windows NT and Novell NetWare servers. The root of SystemView for OS/2 is NetFinity (also known as TME 10 NetFinity in this publication), a member of the SystemView series.

NetFinity provides PC hardware management, discovery, hardware and software inventory and file transfer functions. It is the entry-level product for customers who want to invest in IBM systems management. It provides comprehensive, easy-to-use system management functions at a low cost. NetFinity Services are pre-loaded on some IBM hardware, such as commercial desktops and mobile systems. Moreover, all IBM servers ship with ServerGuide which contains a copy of NetFinity Manager and licenses to allow that manager to be managed remotely. This provides the customer with instant system and asset management capabilities, when they buy IBM systems, at no additional charge. NetFinity and SystemView for OS/2 also come with a built-in DMI browser.

Expanding on these capabilities, SystemView for OS/2 builds upon the NetFinity base with additional capabilities of its own, such as software distribution and preparation, license management and remote control. SystemView for OS/2 provides comprehensive systems management for your PC environment. Automated functions such as pro-active monitoring and event scheduling help lower the cost of system ownership.

SystemView for OS/2 provides the following functions to assist with systems management:

- Real-time monitoring, which allows network managers to discover problems before users do and solve them
- A software process monitor, which enables managers to keep applications up and running and users productive by sending alerts when they are in a non-acceptable state
- Support for DB2/2 and Lotus Notes, which allows operations to re-use configuration and performance data in those familiar formats, thus reducing the user′s learning curve

- A software inventory dictionary of over 3000 titles, which enables SystemView for OS/2 to automatically find the applications users have installed
- Extensive performance monitoring metrics that enable systems administrators to learn about poor performance before the users do and take preventative actions
- A wide variety of automation options that enable users and system administrators to make everyone's life easier

SystemView for OS/2 is especially suited for small- to medium-sized organizations, and some large organizations that do not need the tight integration with enterprise-level management functions addressed by other SystemView managers, such as that provided by the AIX, OS/400 or MVS SystemView products.

The automation options of SystemView for OS/2 are the features that we focus on in this publication.

1.1 SystemView for OS/2 Alerts

SystemView for OS/2 modules use alerts to report a status on SystemView module responsible for monitoring that condition issues an alert, documenting the event and passing it to the Alert Manager.

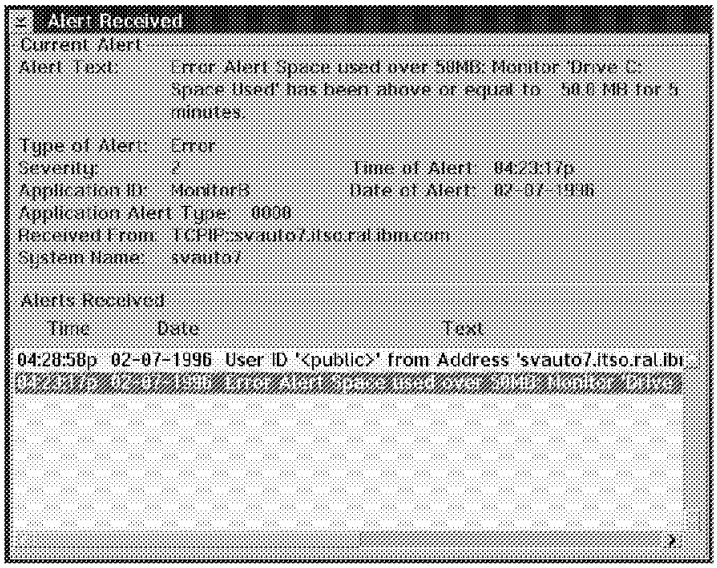


Figure 1. Alert Received Pop-Up Window Sample with Alert Data

Alerts may contain the following information:

- **Alert Text** is a text field containing the name of the alert and any textual description.

  This text can be included in an alert or trap that can be forwarded onto SystemView for MVS or SystemView for AIX. Note that alert information, which gets forwarded to MVS through FFST/2, does not send all the text. Only a small part of the text gets forwarded in the alert.

- **Type of Alert** specifies the application sending the alert and its possible types. The following alert senders are available:

  - System
  - DASD
  - Operating System
  - Application
  - Device
  - Security

  The following alert types may be sent:

  - Failure
  - Error
  - Warning
  - Information

  As an example, you may have an alert type of Application Warning.

- **Severity** is a value from 0 to 7, with 0 being the most severe, used to describe how critical the alert is. When SystemView is installed, the alert processing default will add to the alert log only the alerts with a severity from 0 to 5, and issue a warning pop-up window for alerts with severity 0 to 3. This can be changed in the Action Editor to suit different needs.
- **Application ID** contains the name of the application that generated the alert (up to 8 characters).
- **Application Alert Type** is a numeric value assigned by the issuing application to detail the alert. For example, it could be a return code.
- **System Received From** contains the address of the system from whom the alert was received and the transport protocol it was delivered on.
- **Time of Alert** contains the time the alert was generated.
- **Date of Alert** contains the date the alert was generated.
- **System Name** the name of the system that issued the alert.

This structure allows the alert to carry nearly any type of information about events detected by the SystemView modules or even your own procedures.

1.2 Components That Issue Alerts

The following SystemView for OS/2 components issue alerts:

- Critical File Monitor
- Process Manager
- Remote System Manager
- System Monitor Thresholds
- Security Manager
- Service Manager
- Power-on Error Detect
- Predictive Failure Analysis
- RAID
- Genalerts (for user and application alerts)

1.2.1 Critical File Monitor

The Critical File Monitor allows you to monitor any file and issue alerts when a file is modified, created or deleted.

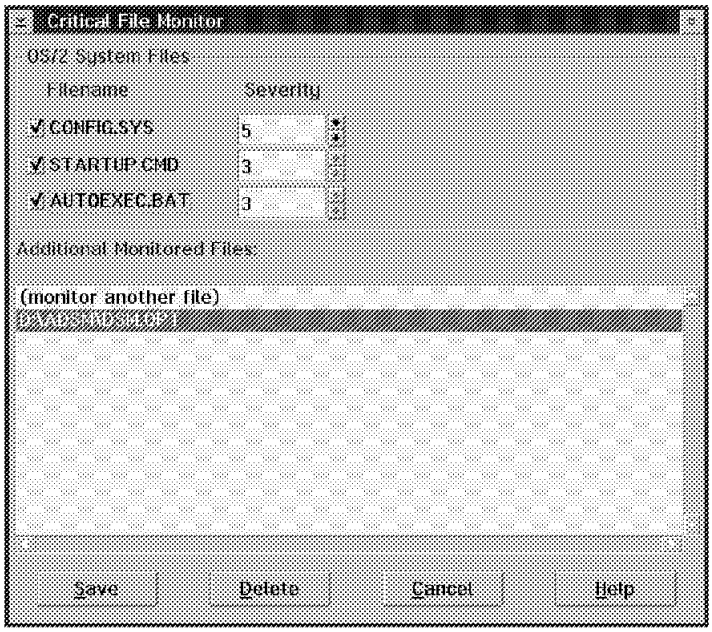


Figure 2. Critical File Monitor Window

You may monitor the default critical files for the platform you are managing, or add any others to the Additional Monitored Files list. The default list displayed by the Critical File Monitor will be different for each operating system that SystemView for OS/2 supports.

1.2.2 Process Manager

The Process Manager is a service present on the SystemView Manager that allows you to monitor processes running locally or on any remotely managed workstation. It may issue alerts notifying the alert service when a program runs, stops, or is not run after a specified time interval. Depending on the system you are managing, the processes monitored may have different characteristics; you monitor NLMs in NetWare and processes in OS/2.

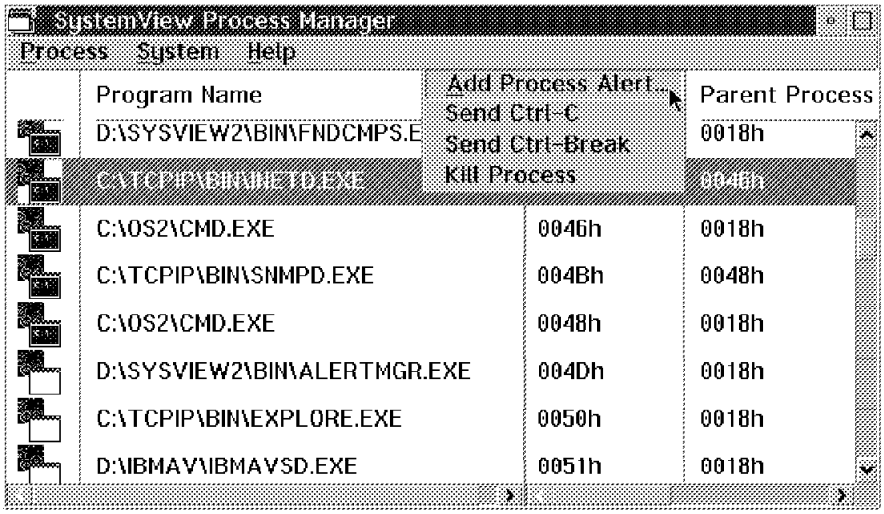


Figure 3. Process Manager Window

Select the process you wish to monitor in the Process Manager window, as shown in Figure 3, and press the right mouse button. Choose **Add Process Alert**.

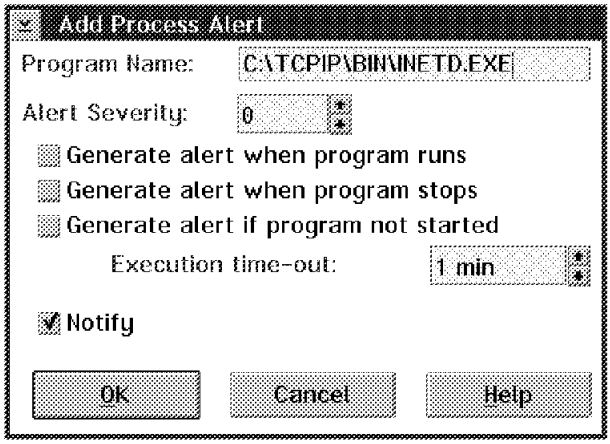


Figure 4. Add Process Alert Window

Specify, in the Add Process Alert window, under what conditions you want the alert to be issued.

1.2.3 Remote System Manager

The Remote System Manager monitors workstations and allows you to receive alerts when a system is offline or online. In other words, if you are monitoring for a system′s off-line status, when the interval passes (that is, specified in its presence check), an alert will flow to the manager. In addition, when it eventually comes online, an alert can also be sent.

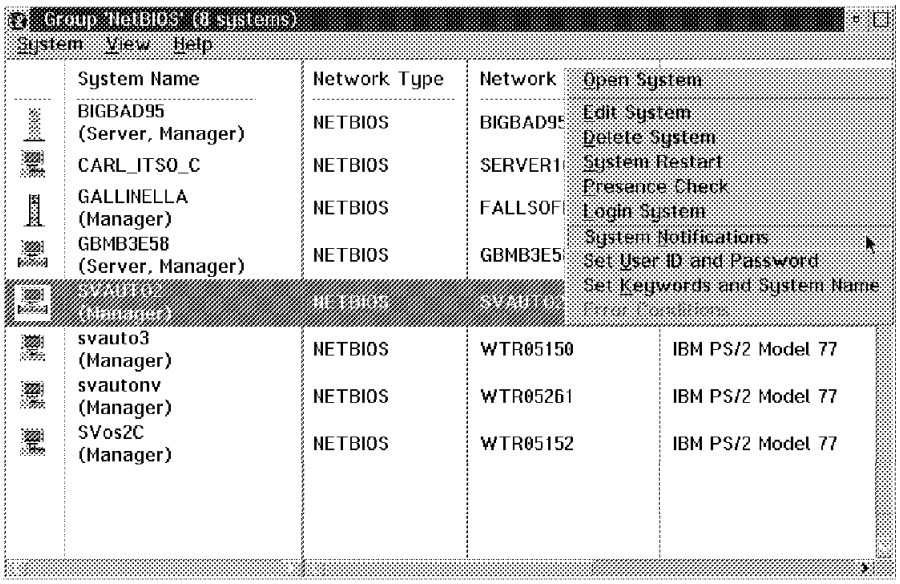


Figure 5. Process Manager Window

Select the workstation you want to monitor and click on it with the right mouse button, as shown on Figure 5. On the context menu, choose **System Notifications**.

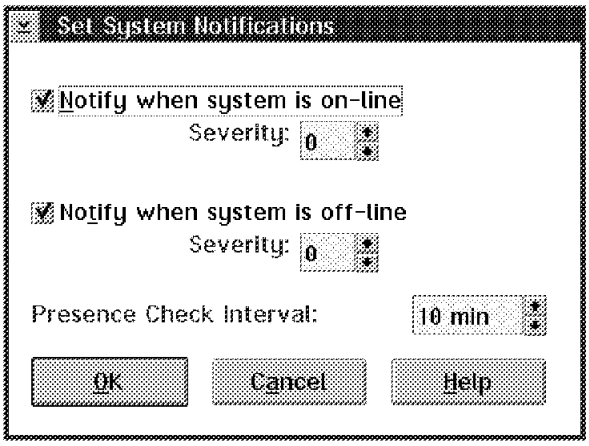


Figure 6. Set System Notifications Window

Check the boxes corresponding to the alert you that wish to receive.

1.2.4 System Monitor

The System Monitor service monitors activity and usage of a wide range of system components (including RAID disks) and may issue alerts when thresholds are reached or exceeded. In addition, when conditions return to a normal state, an alert can also be sent to indicate such a state.

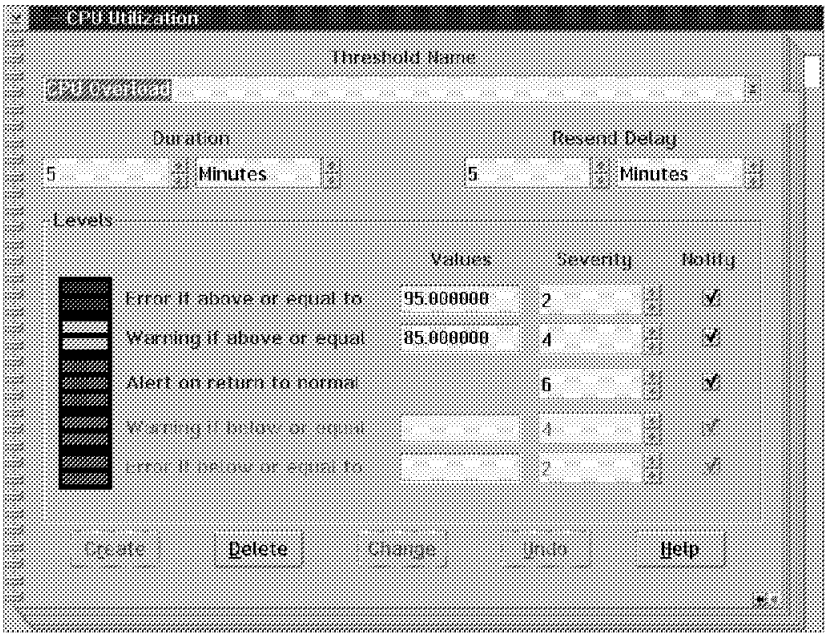


Figure 7. Threshold Notification Notebook Page

The thresholds may be equal, above or below specified values. The alerts sent will notify error, warning and return-to-normal conditions.

1.2.5 Security Manager

The Security Manager generates alerts in response to access attempts (successful or unsuccessful) and to the remote boot function. These alerts are automatically generated and do not require any additional customization.

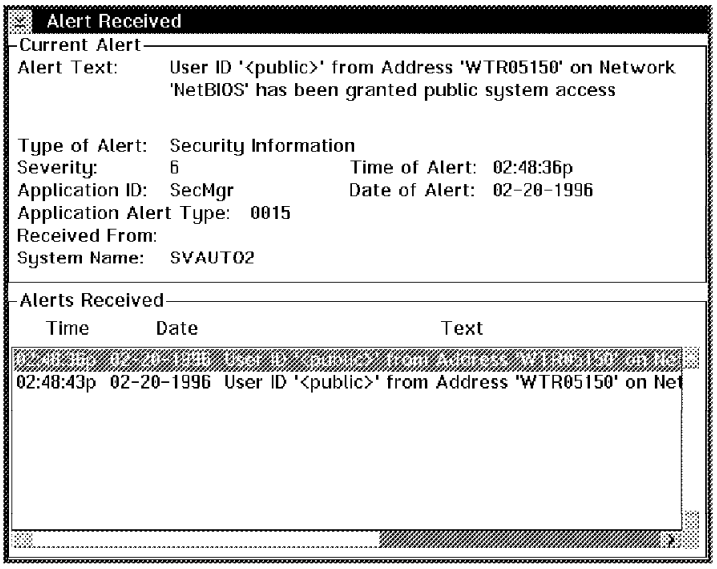


Figure 8. Sample Alert from Security Manager

Figure 8 shows an example of a Security Manager generated alert, informing you that a userid has been granted access to the system.

1.2.6 Service Manager

The Service Manager may generate alerts when any SystemView service (module) is executed from a remote user. To set these alerts to be generated, go to the SystemView Customization notebook; under the General tab, click on **Options**.

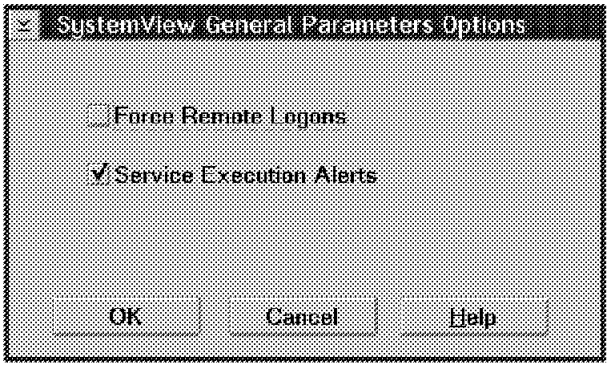


Figure 9. SystemView Configuration Notebook Options Window

Check the **Service Execution Alerts** check box to have Service Manager generated alerts.

1.2.7 Power-on Error Detect

Power-on error detect (POED) allows you to generate alerts when power-on self-test (POST) error messages are received. If your hardware supports POED/POST, you may automate power-on handling by checking (in the POED window) under **Options**, the pull-down menu item **Alert on error**, as shown below.

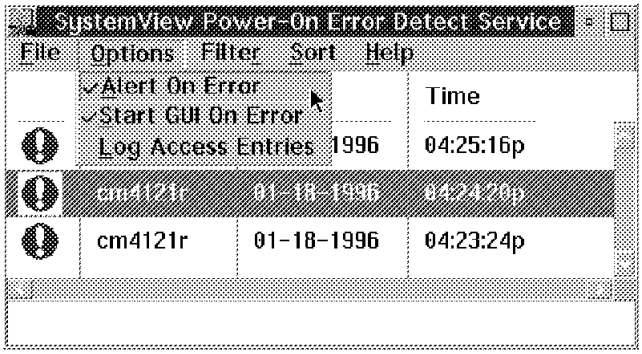


Figure 10. Power-On Error Detect Window

1.2.8 Predictive Failure Analysis

The Predictive Failure Analysis (PFA) service enables you to monitor the functionality of all PFA-enabled disk drives installed locally on your system, or on remote systems within your network. With this service, you will instantly be notified when a PFA-message is generated by a PFA-enabled drive.

You can configure this service to automatically generate an alert when a PFA message is received.

Each PFA-enabled physical drive is represented by an icon in the Predictive Failure Analysis window. The PFA service uses two different icons to help you quickly determine the status of each disk drive. These icons are as follows:

Figure 11. Disk OK Icon

The Disk Ok icon indicates that the drive has not reported any predictive failure analysis messages.

Figure 12. Disk Error Icon

The Disk Error icon indicates that the drive has reported one or more predictive failure analysis messages and may be failing.

On the PFA window you may double-click on a specific drive and check the **Generate Alert** check box. This will cause the Predictive Failure Analysis service to generate an alert when a PFA Error message is reported by the PFA-enabled disk drive. This alert will contain the Alert Text shown in the PFA Options for Drive window (as well as any additional text you have entered in the Additional Text for Alert Log field) and will have the Severity value you have selected in the Severity field.

1.3 GENALERT

We may generate our own alerts using the GENALERT command provided by SystemView for OS/2. GENALERT is located in the SystemView directory and has the following syntax:

```
GENALERT  /T:"text" /APP:id_name /SEV:<0..7> /TYPE:sssttt /ATYPE:hexnum
```

where:

/T:"text" defines the text message describing the alert.

/APP:id_name defines the application ID for the alert (1 to 8 characters).

/SEV:<0..7> defines the severity of the alert (0 = max, 7=min).

/TYPE:sssttt defines the standard type of alert. The sss field describes the ID of the alert:

- UNK - Unknown
- SYS - System
- DSK - Disk or DASD
- NET - Network
- OS_ - Operating System
- APP - Application

- DEV - Device
- SEC - Security

The ttt field describes the class of the alert:

- UNK - Unknown
- FLT - Fault or Failure
- ERR - Error
- WRN - Warning
- INF - Information

/ATYPE:hexnum defines the application-specific alert type as a hexadecimal value between 0000 and FFFF.

Example:

```
GENALERT /T:"***TEST ALERT" /SEV:0 /APP:IBMAV /TYPE:APPWRN
```

The command above generates an alert with the text "***TEST ALERT", severity 0, from application IBMAV and alert type Application Warning. GENALERT generates equivalent alerts to any other SystemView application and is available for the following platforms:

- OS/2
- Windows
- Windows 95
- NetWare

1.4 Alert Flows

The basic alert route begins on the applications that issue alerts (see 1.2, "Components That Issue Alerts" on page 3). These applications send alerts to the alert manager base module when specified conditions are met. The alerts carry information on the condition met and its originator. The alert manager uses action handlers to process alerts, based on an *alert type x alert action* correlation defined by the user. This correlation is configured in the Action Editor GUI, giving the user flexible action conditions (see 1.5, "Action Editor" on page 11). The action handlers may receive alert information from the alert manager in the form of parameters when necessary.

SystemView is extendable regarding alerts in two ways:

- New services can initiate their own alerts to the alert manager base and take advantage of the alert action handlers that are already provided.
- New action handlers can be added, becoming available to the user in the Action Editor, to be used as alert actions.

These new extensions must be done with programming complying to SystemView's object-oriented alert processing.

1.5 Action Editor

Any SystemView alert may trigger an action. You may specify the actions that you want to be performed for each alert in the Action Editor, under the Alert Manager. After clicking on the **Alert Manager** icon (shown in Figure 11 on page 9), click on **Actions** and then **New**. This will start the Action Editor window.

Figure 13. Action Editor Icon

Specify under Alert Conditions the alerts that will trigger the action. The potential actions you can take are as follows:

- Send the alert as TCP/IP mail.
- Send an SNMP alert through TCP/IP to another manager such as NetView for AIX.
- Send an SNMP reset alert.
- Send an alert to an alphanumeric pager.
- Activate a numeric pager.
- Forward the alert to FFST/2.
- Export to a Lotus Notes database.
- Export to a DB2 database.
- Send E-mail using the Vendor Independent Mail interface.
- Clear error condition for sending system.
- Set error condition for sending system.
- Execute minimized command.
- Notify user with a pop-up window.
- Forward the alert to another manager.
- Add the alert to a log file.
- Play a waveform (WAV) file.
- Send DMI indication to DMI service layer.
- Print the alert.

1.6 Passing Alerts on to Other Operating Systems

- AIX - Using the alert action to send an SNMP alert through TCP/IP will forward this alert as a trap to an SNMP manager such as NetView for AIX.

  The destinations will be set up in your OS/2 TCP/IP V3.0 trap destinations table. You will need to make sure that you have the correct community name.

- OS/2 - You can also forward the alert as a trap to NetView for OS/2 since it is an SNMP manager too.

- MVS - You can forward the alert to FFST/2 and then use an LU 6.2 connection setup in CM/2 to send the alert to NetView for MVS.

  You will need to have set up the CM/2 Service Point application as well as Remote Operations. Once this is all set up, you can also use RUNCMDs from NetView for MVS to send commands back to SystemView for OS/2.

Chapter 2. AntiVirus

This chapter shows an example of automated problem resolution when a virus is detected on the following platforms:

- OS/2 Warp Connect
- Windows 95
- DOS 7.0 with Windows 3.1
- NetWare
- Windows NT

The automated procedure periodically runs the IBM AntiVirus software on the machines to be monitored to check for virus infection. Automated actions are triggered when one of the following is true:

- A virus is found.
- The IBM AntiVirus software fails to run.
- The IBM AntiVirus software runs without signaling *No virus found*.

If a virus is found, the process generates a SystemView for OS/2 alert to remove the machine from the network, notify the LAN Administrator, and to immediately run the IBM AntiVirus software on other possibly infected machines.

The two other conditions send an E-mail message to the LAN Administrator, specifying the error condition with logs from the IBM AntiVirus software.

2.1 System Environment

This scenario used the following environment:

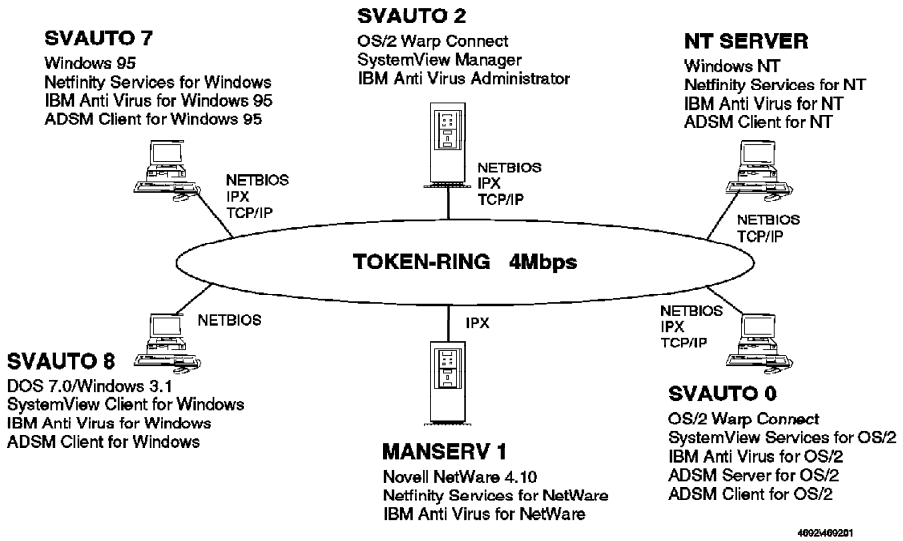


Figure 14. System Environment

SystemView and NetFinity clients work with the SystemView Manager for OS/2. SystemView supports only OS/2 and DOS/Windows clients, therefore the NetFinity Client will be used in the remaining platforms (Windows 95, Windows NT and NetWare).

We assumed for this scenario that all the software had already been installed, except for the following:

- NetFinity Services for Windows 95
- IBM AntiVirus for Windows 95
- ADSM Windows 95 Client
- NetFinity Services for NetWare
- IBM AntiVirus for NetWare

DOS 7 supports the REXX programming language. We make use of REXX programs on both DOS/Windows and Windows 95 clients, so be sure you have DOS 7 installed with REXX support on these workstations.

2.2 Windows 95 Client Preparation

The following software was used in this scenario:

- NetFinity Services for Windows 95
- IBM AntiVirus for Windows 95
- ADSM Windows 95 Client

2.2.1 Install NetFinity Services for Windows 95

NetFinity can be installed from diskettes, CD or from a LAN drive. We installed it from a CD. To install, click on **My Computer** on the Windows 95 desktop. The icon on the desktop looks like Figure 15.

Figure 15. My Computer Icon

After you click on it, a window will open up. Insert the NetFinity CD into the CD-ROM drive and choose the icon representing your CD-ROM drive in the My Computer window. Our CD-ROM drive was located on our D: drive. Also, notice that in Figure 16 on page 15 the label for the CD appears under the drive.

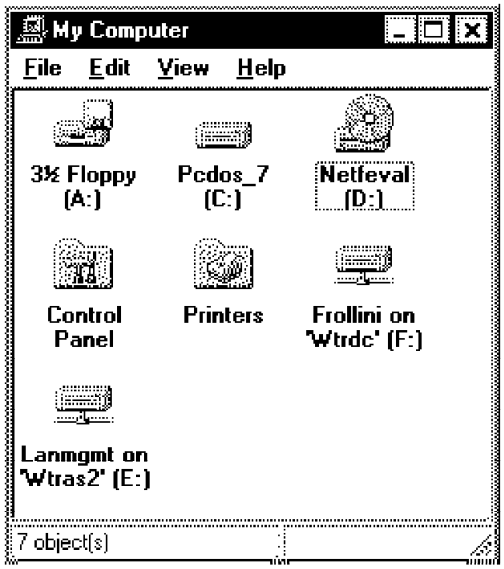


Figure 16. My Computer Window

Double-clicking on the **Netfeval D:** drive opens a window and shows the contents of the CD. There are folders containing documentation, as well as code for the various supported platforms. Click on the **Windows** folder. This folder contains both the manager and client code for Windows. Choose the **Services** icon. The following window will appear:

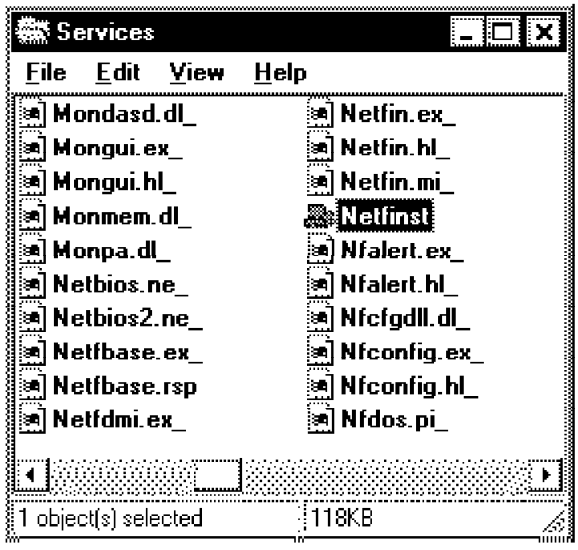


Figure 17. NetFinity Services for Windows CD Directory

Click on the **Netfinst** icon to start the installation process. In our machine, all screen activity stopped and after approximately 40 seconds, the following NetFinity installation window appeared.

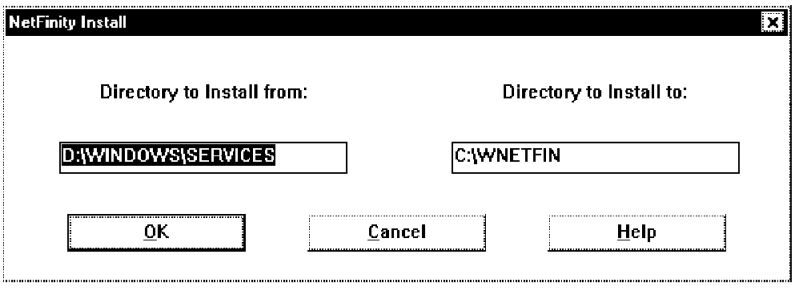


Figure 18. NetFinity Install Window

Accept or alter the values for the source and destination directory for NetFinity. Always use full path names on each field, according to where you would like to install NetFinity *from*, and where you would like to install NetFinity *to*. Press the **OK** button to continue.

This will bring up the following window:

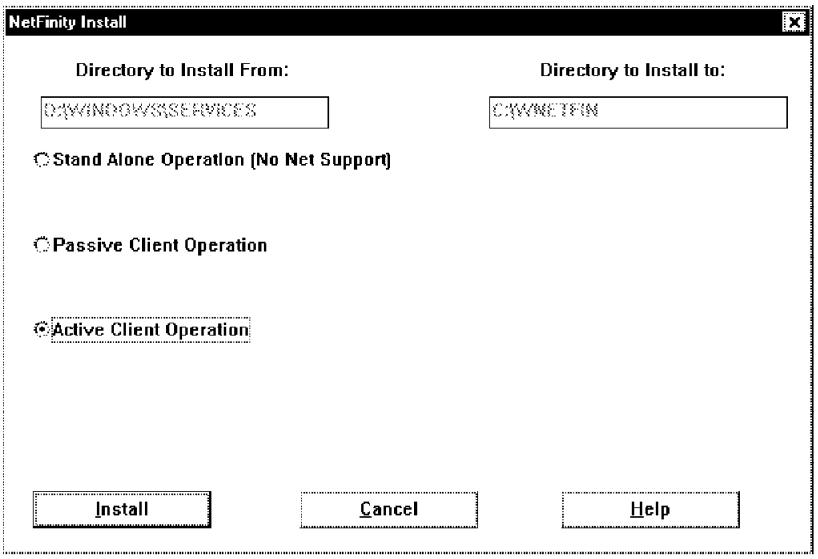


Figure 19. Second NetFinity Install Window

Stand Alone Operation installs NetFinity without any network support, thus enabling only local functions.

Passive Client Operation enables remote management functions by the SystemView Manager, with limited functions available for the local user.

Active Client Operation installs NetFinity with all functions available both locally and remotely.

We chose **Active Client Operation** and selected **Install**.

The NetFinity Install - Installing... window will appear, showing the status of the installation process.

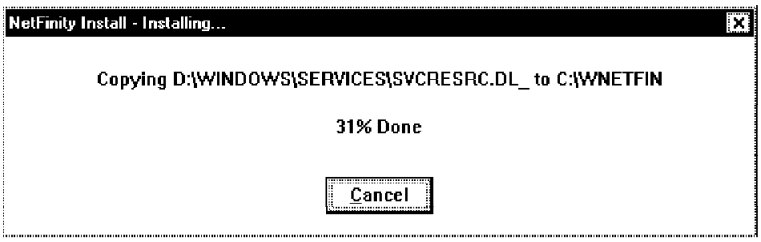


Figure 20. NetFinity Install - Installing... Window

When the progress reaches 100%, the window disappears. The installation program now updates the Startup folder, creates the NetFinity folder, starts the Network Driver Configuration program and, in a new window, prompts you whether or not to update the file AUTOEXEC.BAT.

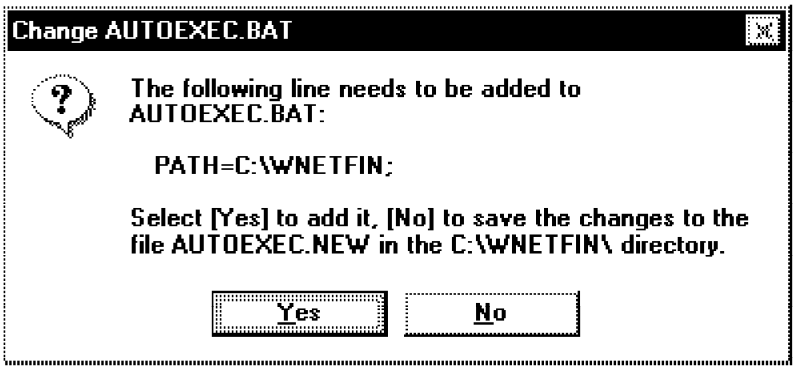


Figure 21. Change AUTOEXEC.BAT

NetFinity needs its directory inserted in the PATH statement within AUTOEXEC.BAT. Click on **Yes** to complete the update.

The NetFinity Install Complete! window appears as follows:

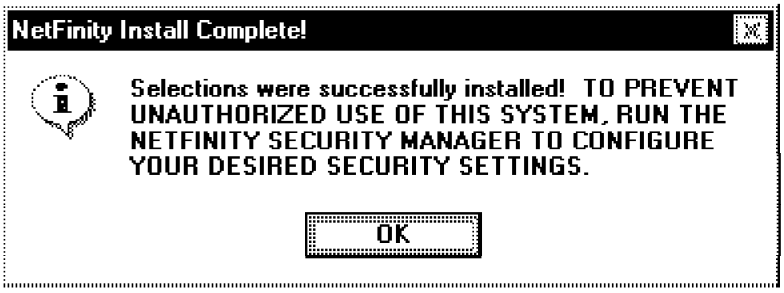


Figure 22. NetFinity Install Complete! Window

NetFinity installs a <PUBLIC> userid by default in the Security Manager ini file. This user ID allows any user to perform any of the NetFinity functions available remotely without a password. It is recommended to restrict this access as soon as you finish the NetFinity installation process to prevent unauthorized use of the system.

After you press **OK**, the NetFinity installation process is finished. Customize the network driver configuration using the Network Driver Configuration window started by the installation process:

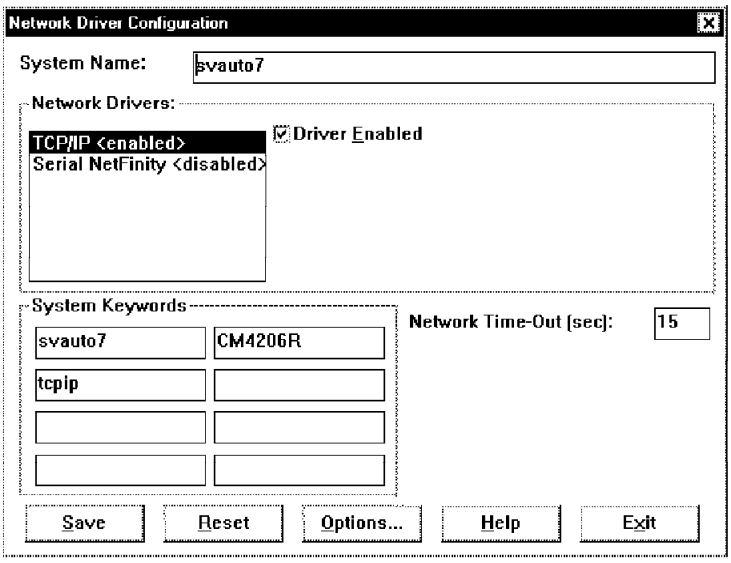


Figure 23. Network Driver Configuration Window

Enter the name the SystemView Manager will use to identify this machine in the System Name field.

Select from the list of available Network Drivers listed in the Network Drivers field. To enable a driver, check the **Driver Enabled** check box next to it. We have enabled the TCP/IP driver only in this scenario, but it is possible to enable others if they are on the system. In this case, NetBIOS was not installed on the system, so it was not presented as an option. For NetBIOS and Serial communication, you need additional information such as a network address. Please see the *IBM NetFinity Services for Windows User's Guide* manual for details on enabling different drivers.

Enter any keywords used by the SystemView Manager to group workstations in the System Keywords fields. Keep in mind that the keywords are case-sensitive. For example, svauto7 is not the same as svAuto7.

Type, in the Network Time-Out field, the number of seconds that the SystemView Manager should wait for responses from this machine. If your network traffic is high, you might want to increase this value.

Select **Save** to save your configuration. The window in Figure 24 will appear.

Figure 24. Configuration Warning to Restart NETFBASE.EXE

NETFBASE.EXE is NetFinity's equivalent to the SystemView Support Program. Every time it is started, it reads the configuration information defined in the Network Driver Configuration window. It is taking this information from the INI

files. Therefore, any changes to the network configuration will only take place after you restart NETFBASE.EXE.

The NetFinity installation process updates the Startup folder adding its Network Interface program and the ECC Memory Setup program. The latter is only installed in systems with ECC Memory. Our system, a PS/2 Model 9595 had ECC Memory. If your machine does not have ECC Memory, the ECC Memory program will not be added to your Startup folder. The install process also creates the NetFinity folder.

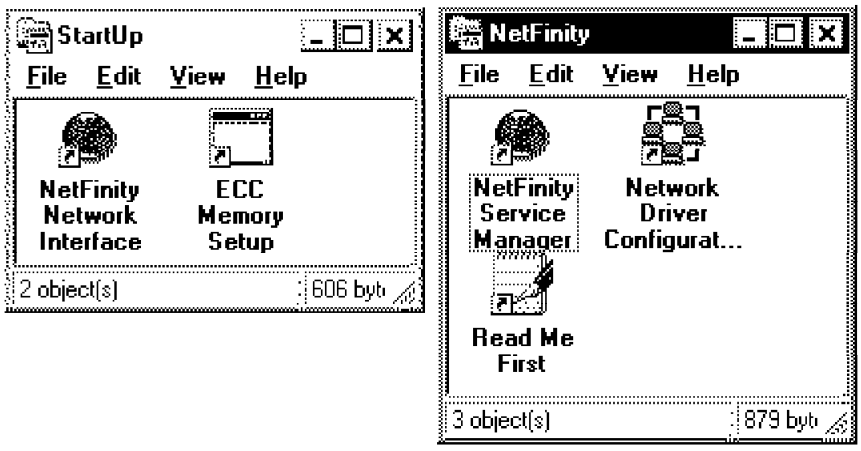


Figure 25. Folders Created/Updated by the Installation Process

Finally, the Start Menu is also updated with the NetFinity folder, as you can see in Figure 26.

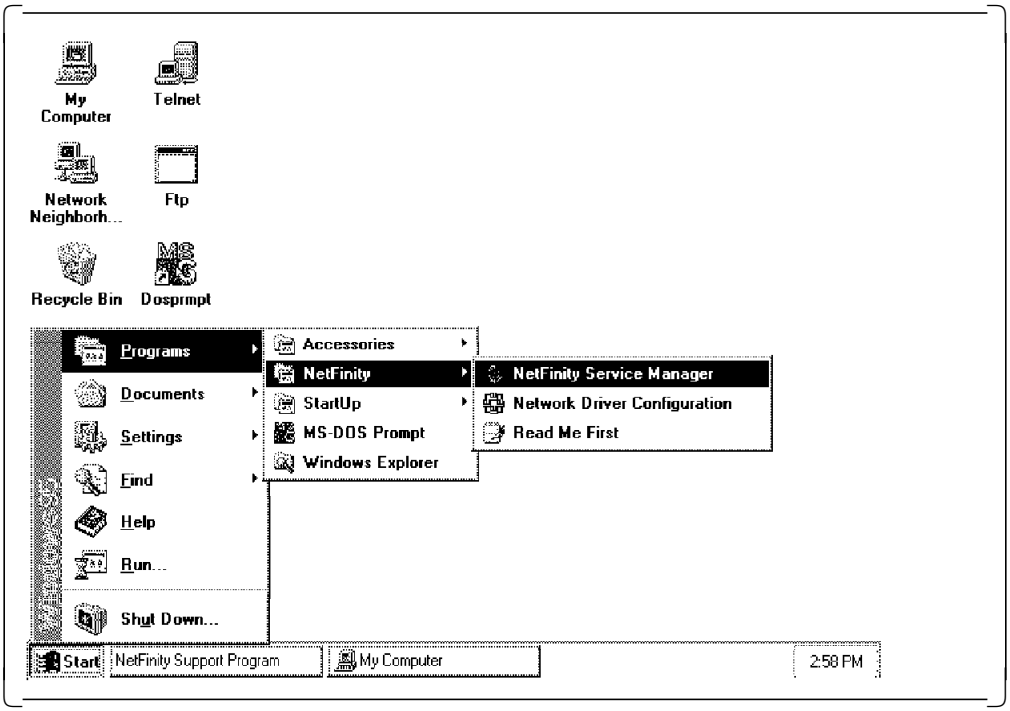


Figure 26. Start Menu Path to the NetFinity Folder

Reboot your machine by clicking on the **Shut Down** button from the Windows 95 start menu. Choose the option **Restart the Computer?** and select **Yes** to boot the machine.

After the boot, you should see the NetFinity Support Program window starting up and automatically minimizing itself when its network interfaces are activated successfully.

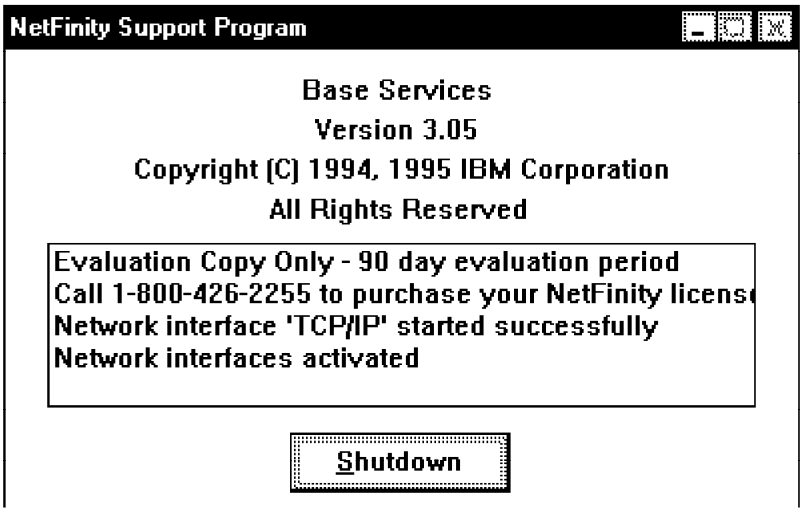


Figure 27. NetFinity Support Program Window

This completes the steps for the NetFinity client installation. The NetFinity functions are available from the Startup Menu, as shown in Figure 26 on page 19. To start the NetFinity Services GUI, choose the **NetFinity Service Manager** icon.

2.2.2 Install IBM AntiVirus for Windows 95

We installed IBM AntiVirus for Windows 95 from a LAN redirected drive. It can also be installed from diskettes. To install IBM AntiVirus for Windows 95 from the LAN, run the install program from the Run... option located in the Start Menu:

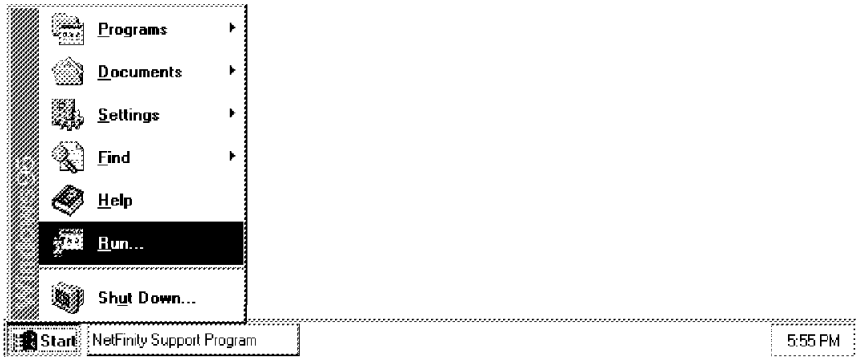


Figure 28. Run... Option in Start Menu

IBMAV was located in the ibmav95 directory of the F: drive. Type the full path name of the IBM AntiVirus setup program and select **OK**.

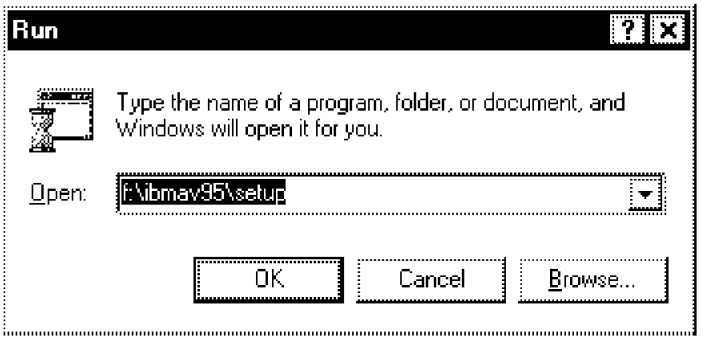


Figure 29. Input the Full Path Name for IBM AntiVirus Setup

The installation program starts with an initialization window:

Figure 30. IBM AntiVirus Install Initialization Window

Select **Next** when you are prompted with the welcome window as shown in Figure 31.

Figure 31. IBMAV Install Welcome Screen

After clicking on **Next**, the following screen appears:

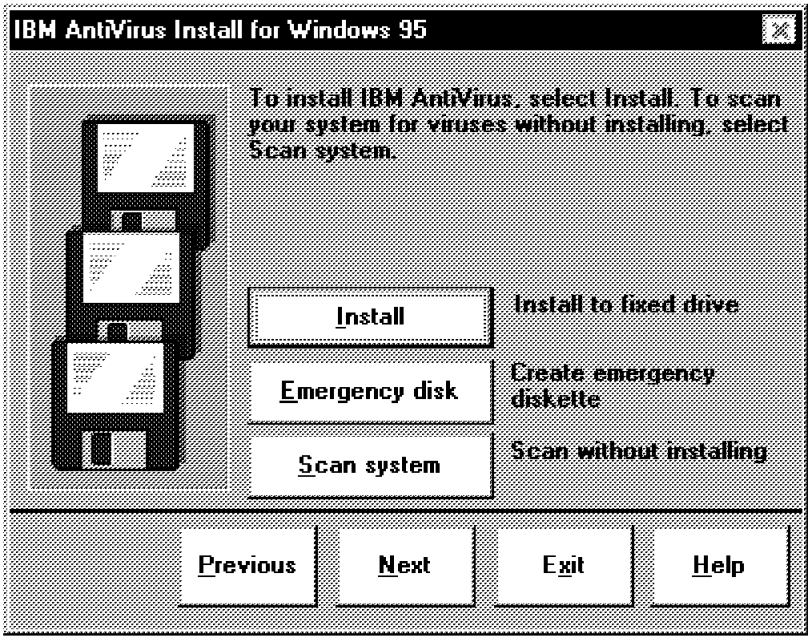


Figure 32. IBMAV Install Selection Screen

You may choose the following:

- **Install** to start the installation process.
- **Emergency Disk** to create a set of emergency diskettes. These are bootable DOS diskettes with IBMAV to be used in systems that cannot boot from the hard disk due to a virus problem.
- **Scan System** to start IBM AntiVirus to scan the system for viruses without installing it on the hard drive.

Select **Install** to continue the installation. On the next window, update the Destination Directory field with the directory name where you want IBM AntiVirus to be installed. Then select **Next**.

Then choose **Custom** so you can change the installation parameters to suit your environment. If you choose **Express**, the installation process will install IBM AntiVirus with its default settings. After making the selection, choose **Next**.

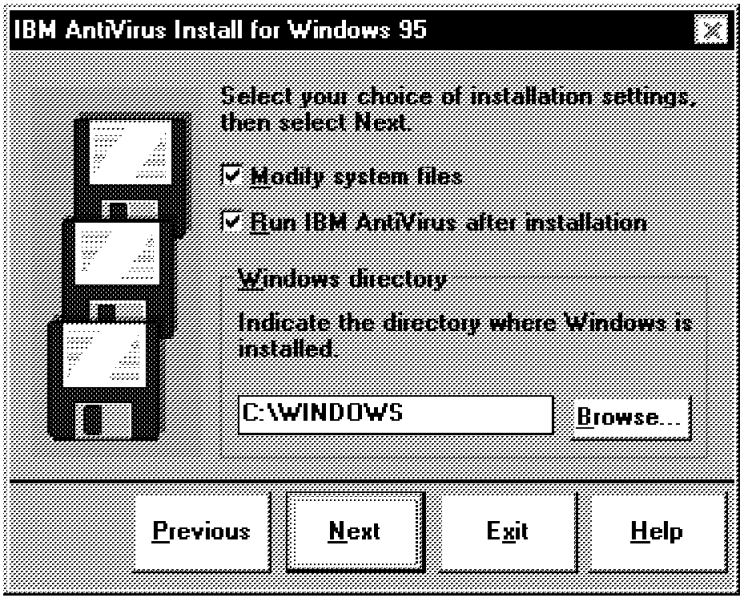


Figure 33. Installation Settings Window

Highlight the check box **Modify system files**. This will cause the install program to update the AUTOEXEC.BAT and WIN.INI files with IBMAV settings. Highlight the **Run IBM AntiVirus after installation** check box to automatically run IBM AntiVirus when the installation process is finished.

Type the name of the directory where Windows is installed in your system in the Windows directory field, and then select **Next**.

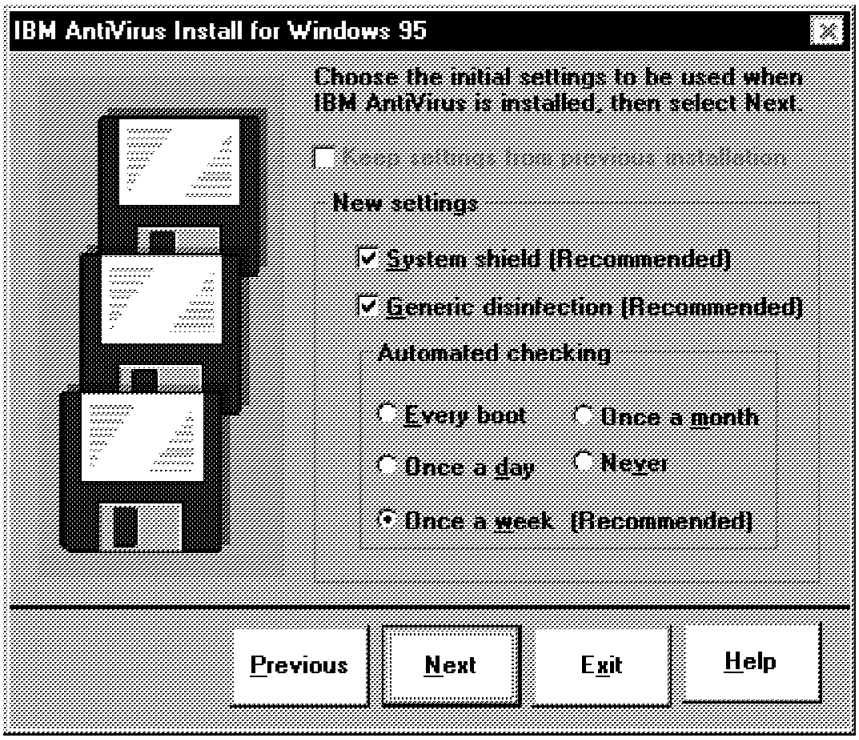


Figure 34. IBMAV Initial Settings Setup Window

Use this window to customize IBMAV's parameters.

The Keep settings... check box will only be available if you already have IBM AntiVirus installed on your system. It allows you to keep your previous configuration.

System shield enables a series of functions for active monitoring of the system. For example, monitor programs running in DOS warn you when virus activity occurs, or check files when they are opened.

Generic Disinfection allows IBM AntiVirus to gather disinfection data to be used later in eventual cleanup procedures.

Specify in the **Automated Checking** field the frequency you would like IBM AntiVirus to automatically run, using its own scheduling system.

After making your selections, choose **Next**.

On the next window, select **Install** to continue with the installation, or click on **Previous** to review any of the install parameters previously entered. Figure 35 is displayed showing the status of the installation process.

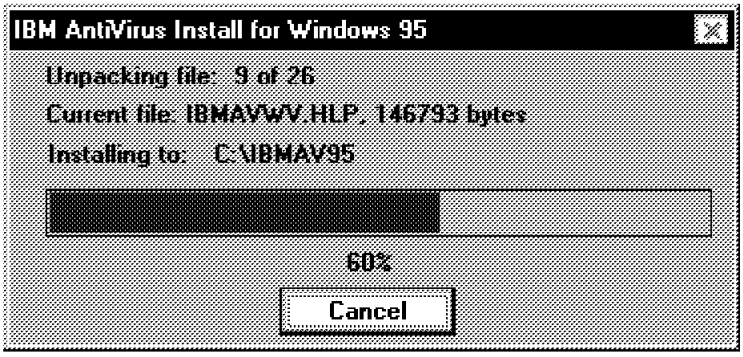


Figure 35. IBMAV Installation Status Window

The following window shows the system files modified by the install process. The install process backs up the original files in case you need to restore your system to its previous state.

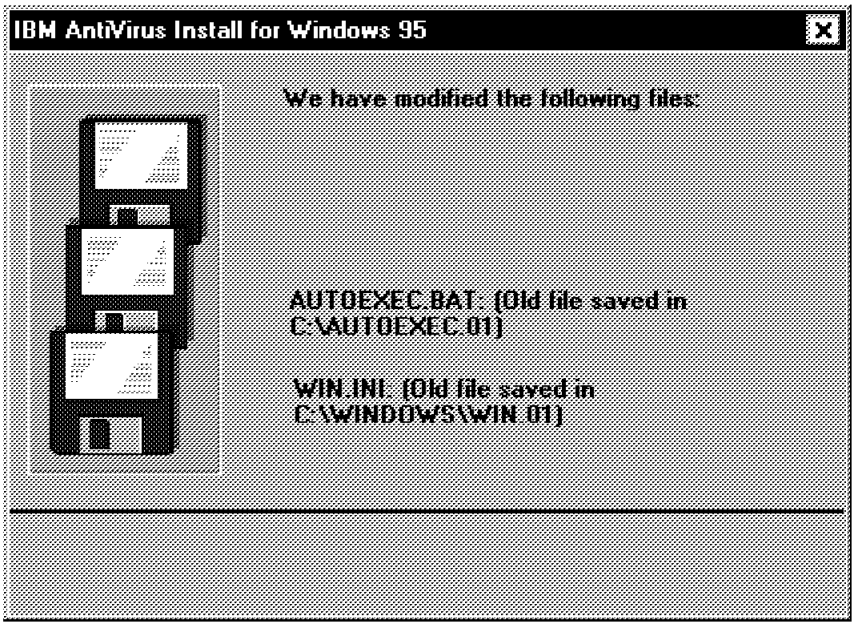


Figure 36. Files Modified by the IBM AntiVirus Install Process

The installation process performs the following modifications to system files:

- Added to AUTOEXEC.BAT:

  C:\IBMAV95\IBMAVSH /FOO to load the initial part of the IBM AntiVirus System Shield

- Added to WIN.INI to automatically start IBMAV:

  C:-IBMAV95-STARTTIM.PIF program is added to the RUN= statement

  The installation program also updates the Start Menu, adding IBMAV under the Programs folder.

After a few seconds, the Installation Complete window appears. You have finished installing IBM AntiVirus for Windows 95. When you select **OK**, the install process will automatically start IBMAV, according to the options you specified in Figure 33 on page 23. After IBM AntiVirus runs, the window in Figure 37 prompts you to reboot your machine to make the changes valid.

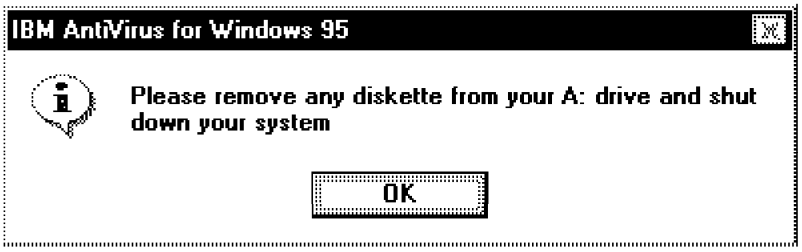


Figure 37. Shut Down the System to Make Changes Valid

Selecting **OK** will not reboot your system; you have to do it yourself by selecting the **Shut Down** option in the Windows 95 start menu.

2.2.3 Install ADSM Windows 95 Client

During the production of this redbook, the ADSM Windows 95 Client was not yet generally available. We used a beta version of the product. Its installation process consisted of the following:

- Copying the necessary files into a target ADSM directory in the client machine
- Adding the C:-WINDOWS-SYSTEM directory to the PATH statement in AUTOEXEC.BAT
- Customizing the DSM.OPT file
- Starting the ADSM Windows 95 Client

The C:-WINDOWS-SYSTEM directory must be added to the PATH statement in AUTOEXEC.BAT. This is because on Windows 95, the 32-bit Windows Sockets DLL, wsock32.dll, resides in that directory. By default the C:-WINDOWS-SYSTEM directory is not included in the default Win95 search path, so it *must* be added before attempting to run the client. Make sure you boot the machine after the PATH statement update.

The following files were copied:

```
dscameng.txt    ----    NLS Message Repository
dsm.opt         ----    Sample client options file
dsm32.exe       ----    Win32 Backup/Archive GUI client
dsmadmc.exe     ----    Command line administrator client
dsmc.ico        ----    Icon file for B/A command line client
dsmc32.exe      ----    Win32 Backup/Archive Command Line client
dsmnt.hlp       ----    GUI client help file
dswadm.ico      ----    Icon file for admin client
ntcons.exe      ----    Trace facility console
readme.nt       ----    Readme for v2.1.0.2 NT client
readme.w32      ----    This file
bwcc32.dll      ----    DLL for ADSM
```

Our DSM.OPT file was customized as follows:

```
NODEname          svauto7
COMMmethod        TCPIP
TCPServeraddress  9.24.104.220
COMPression       ON

Exclude "*:\...\adsm.log"
Exclude "*:\EA DATA. SF"
Exclude *:\...\*.swp
Exclude *:\...\win386.swp
Exclude "*:\...\Icon?"
Exclude "*:\...\ICON?"
Exclude *:\...\386spart.par
Exclude *:\...\*.trc
Exclude *:\...\pagefile.sys
Exclude *:\...\*.par
Exclude *:\...\*.sym
Exclude *:\...\*.obj
Exclude *:\...\*.csm
Exclude *:\...\*.dsk
Exclude *:\...\*.pch
Exclude *:\...\SYSTEM32\CONFIG\*.*
Exclude *:\...\SYSTEM32\CONFIG\...\*
Exclude C:\IBMBIO.COM
Exclude C:\IBMDOS.COM
```

Figure 38. DSM.OPT File

Start the ADSM Client by clicking on the **Dsm32** icon contained in the directory ADSM is installed. Select **OK** on the welcome screen and type your ADSM client password when prompted. The following window will appear:

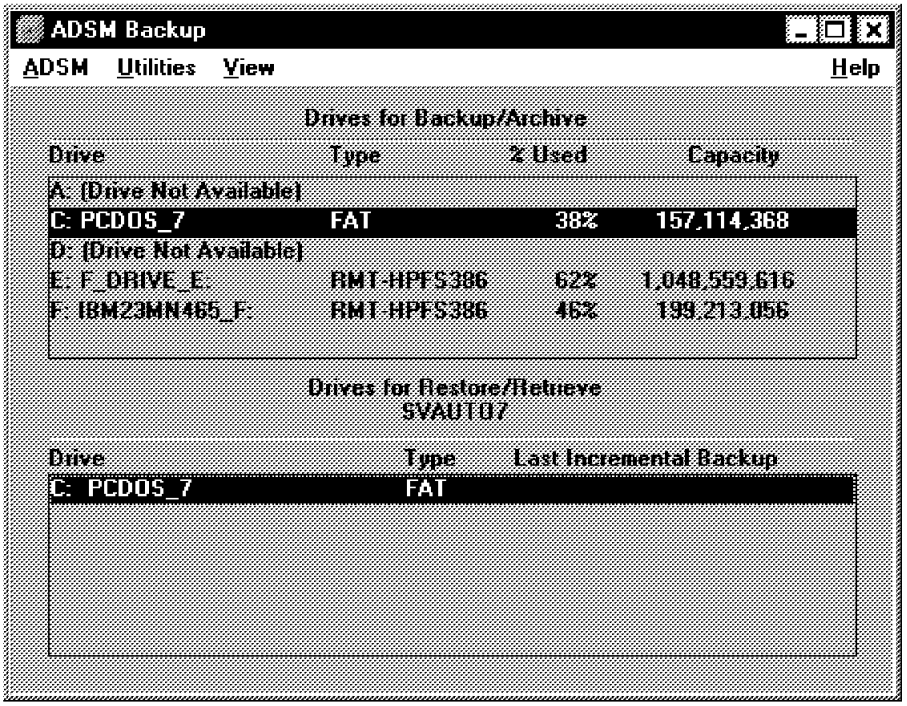


Figure 39. ADSM Windows 95 Client Window

2.2.4 Customize SVAUTO7 for the Automated Process

With the necessary tools properly installed, start customizing the machine for the automated process.

1. Set IBM AntiVirus to run on a regular schedule.
2. Set IBM AntiVirus to issue an alert when a virus is found.
3. Set NetFinity Services to forward alerts to the SystemView Manager.
4. Schedule SystemView to check if IBM AntiVirus has run.

2.2.4.1 Set IBM AntiVirus to Run Periodically

This step can be executed at the time of installation of the IBM AntiVirus for Windows 95 software. See Figure 34 on page 23. If this was not set during the installation, use the IBM AntiVirus GUI to set up the parameters.

Under the IBM AntiVirus GUI, choose **Setup** from the menu bar, then **Automated check...** from the pull-down menu.

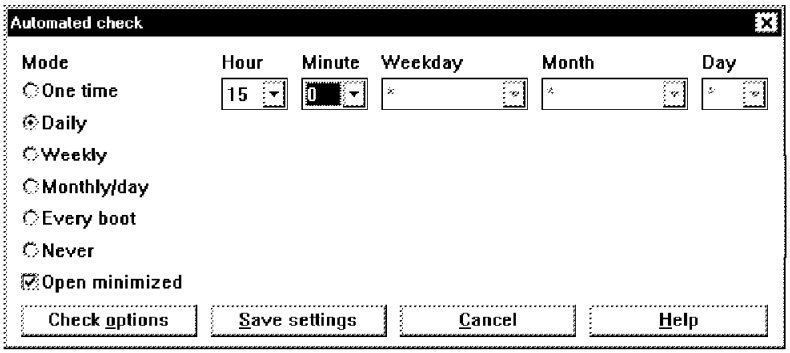


Figure 40. Automated Check Window

Select **Daily** under the Mode field to have IBM AntiVirus run every day at a specified time. Input the time IBM AntiVirus will run in the Hour and Minute fields. Highlight the **Open minimized** check box for IBM AntiVirus to run in the background. Click on **Save settings** to save the settings. Select **OK** on the window that follows that and then click on **Cancel**.

The IBM AntiVirus GUI must be closed for the Automated Checking to occur.

2.2.4.2 Set IBM AntiVirus to Issue an Alert When a Virus Is Found

IBM AntiVirus has an advanced option where you can specify any command to be issued as if it were in a command line. Administrative profiles allow you to control which advanced functions of IBM AntiVirus are available to the user. Therefore, the profiles may be customized with the desired command.

The command to generate an alert is called genalert and it resides in the SystemView directory. It can also be found in the NetFinity executable directory. The syntax of the genalert command is:

```
GENALERT  /T:"text" /APP:id_name /SEV:<0..7> /TYPE:sssttt /ATYPE:hexnum
```

where:

/T:"text" defines the text message describing the alert.

/APP:id_name defines the application ID for the alert (1 to 8 characters).

/SEV:<0..7> defines the severity of the alert (0 = max, 7=min).

/TYPE:sssttt defines the standard type of alert. The sss field describes the ID of the alert:

- UNK - Unknown
- SYS - System
- DSK - Disk or DASD
- NET - Network
- OS_ - Operating System
- APP - Application
- DEV - Device
- SEC - Security

The ttt field describes the class of the alert:

- UNK - Unknown
- FLT - Fault or Failure

- ERR - Error
- WRN - Warning
- INF - Information

/ATYPE:hexnum defines the application-specific alert type as a hexadecimal value between 0000 and FFFF.

Example:

```
GENALERT /T:"***TEST ALERT" /SEV:0 /APP:IBMAV /TYPE:APPWRN
```

The above command generates an alert with the text "***TEST ALERT", severity 0, from application IBM AntiVirus and alert type Application Warning. The genalert generates equivalent alerts for any other SystemView/NetFinity application.

Customize the IBM AntiVirus Administrative profile to execute the genalert command when a virus is found. Administrative profiles are contained in the ADMIN.PRF file in the IBM AntiVirus directory. To modify an Administrative profile, you must copy it to your Managing station and start the IBM AntiVirus Administrator GUI.

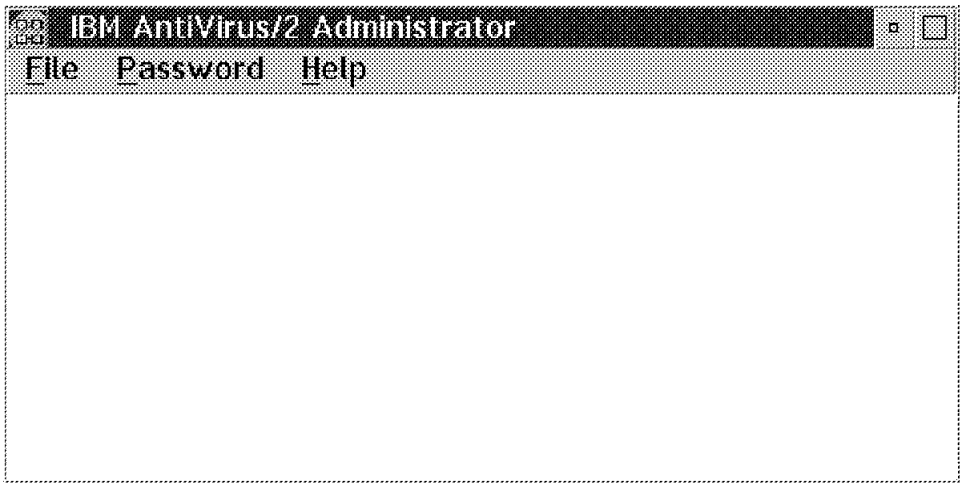


Figure 41. IBM AntiVirus Administrator Graphical User Interface

Choose **File** from the menu bar and then **Open** from the pull-down menu to open a profile. Enter the profile's full path name and select **OK**. The following window appears:

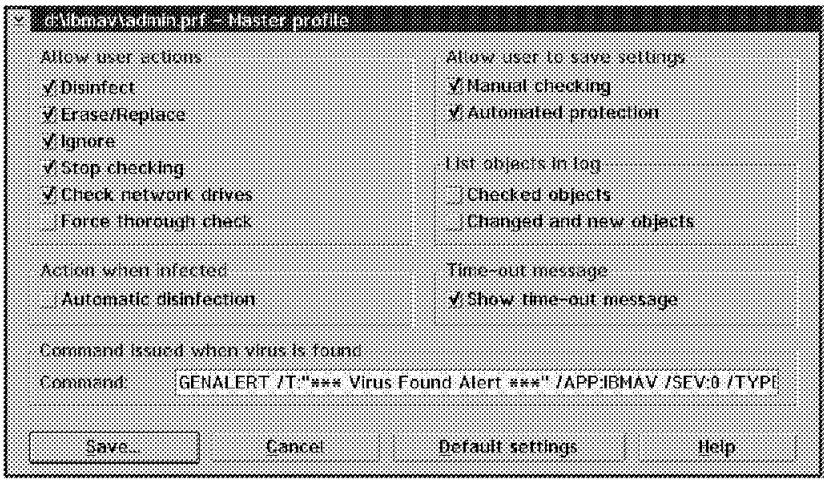


Figure 42. Administrative Profile Setup Window

Many options can be set in this window, as follows:

- Whether or not the user will be authorized to disinfect their own machine when a virus is found.
- An option can be set to authorize the user to scan network drives for a virus.

Make sure the **Automated protection** check box under the Allow user to save settings field is highlighted; otherwise, you will not be able to perform step 2.2.4.1, “Set IBM AntiVirus to Run Periodically” on page 27.

Type the GENALERT command into the *Command issued when virus is found* field. The command used in our scenario was:

```
GENALERT /T:"*** Virus Found Alert ***" /APP:IBMAV /SEV:0 /TYPE:APPWRN
```

This command will issue an alert with the text "*** Virus Found Alert ***", from application IBM AntiVirus, severity 0 and alert type Application Warning.

Click on **Save**, type the IBM AntiVirus Administrator's password, and then select **OK.** Exit the IBM AntiVirus Administrator GUI. You may now use this updated profile in the machine to be monitored.

Note:

Administrative profiles must only be changed by the IBM AntiVirus Administrator. Administrative profiles have internal checksums which make them invalid when altered by anyone other then the IBM AntiVirus Administrator GUI.

2.2.4.3 Forward NetFinity Alerts

We found a modification to genalert on the NetFinity FTP anonymous machine, which allows you to specify a parameter on the GENALERT command to place the network address of the machine where you would like the alert to be sent. Check your GENALERT documentation, and if you have that capability, you may skip this step. Just complement the GENALERT syntax in 2.2.4.2, “Set IBM AntiVirus to Issue an Alert When a Virus Is Found” on page 28 with the network address.

To set NetFinity Services to forward alerts to the SystemView Manager, start the NetFinity Service Manager GUI. Then, double-click on the **Alert Manager** icon. This will bring you the Alert Log window:

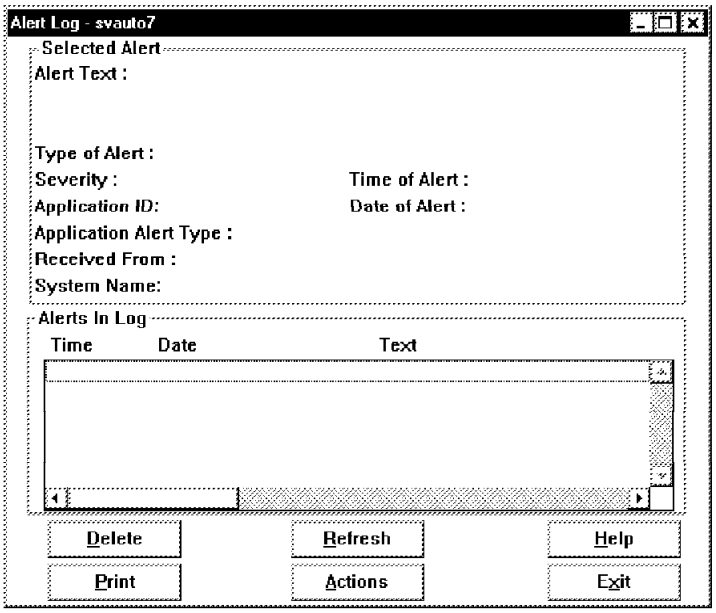


Figure 43. Alert Log Window

The Alert Log window contains all of the alerts received by NetFinity from its own applications. These can be things such as the Critical File Monitor, alerts from thresholds from the System Monitor, or other alerts forwarded from other NetFinity/SystemView machines. In addition, alerts generated by the GENALERT command will show up in the log.

Click on **Actions** to determine what actions NetFinity will take when our specific Anti-Virus alert arrives. On the Alert Actions window, click on **New**. This will bring you to the Action Editor.

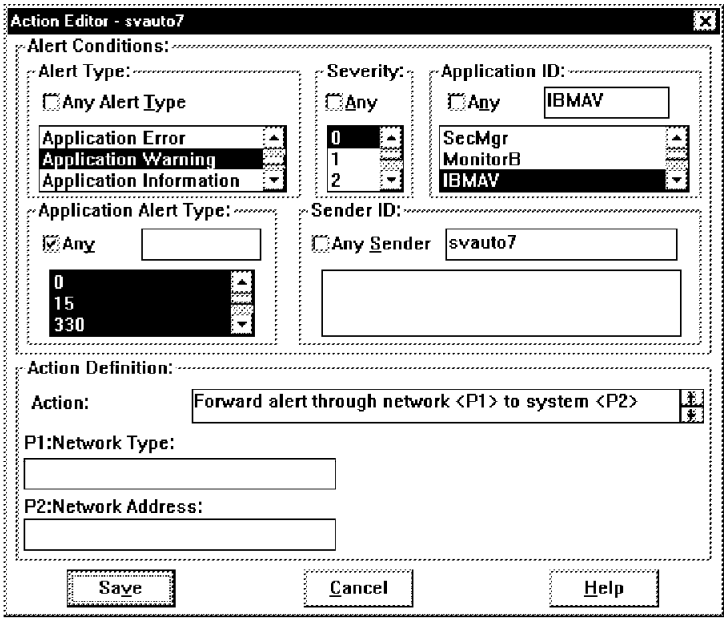


Figure 44. Alert Action Editor

Specify under Alert Conditions what alert parameters will trigger the automated actions. As specified in 2.2.4.1, “Set IBM AntiVirus to Run Periodically” on page 27, our Alert Type is Application Warning, Severity is 0 and the Application ID is IBMAV. The Application Alert ID is not set, so highlight the **Any** check box. The Sender ID should be our machine name, SVAUTO7.

Specify under Action Definition what NetFinity should do when the above specified alert arrives. Browse through with the arrow keys in the Action field until you find the **Forward alert through network <P1> to system <P2>** option. Click on this option.

This will provide you with two additional fields: P1: Network Type: and P2: Network Address:. Input what network protocol NetFinity should use to send this alert in the P1: Network Type: field. This network protocol must have been previously enabled in the NetFinity Driver Configuration, as shown in Figure 24 on page 18, and must also be enabled on the SystemView Manager.

Type the network address of the SystemView Manager in the P2: Network Address: field. This network address can be found in the SystemView Manager by starting the SystemView Service Manager and then choosing the Remote System Manager service. Under All Systems, you will be able to get a detailed view of the workstations and check all of their protocols and addresses. All Systems was a category that we created to show all of the SystemView and NetFinity systems that our manager could discover.

In our scenario, our Network Type is TCP/IP, and the Network Address corresponding to our SystemView Manager is 9.24.104.222. After you fill in the fields, select **Save** and confirm the new action created. You will see the new action just created appear in the Alert Actions window. You may exit the Alert Manager now. You have finished setting NetFinity Services to forward alerts to the SystemView Manager.

2.2.4.4 Schedule SystemView to Check IBM AntiVirus

This step can be achieved in a number of ways. The process we found best is described as follows:

Our main objective is to check to see whether IBM AntiVirus ran OK. This means that no virus was found and IBM AntiVirus had a successful run. IBM AntiVirus logs its last run status on the CURRENT.LOG file. Our procedure will check the CURRENT.LOG file for possible success or error situations. It will also check if CURRENT.LOG has today′s date, to assure IBM AntiVirus was run as scheduled.

```
/* REXX for Windows 95 */
Trace off
Say "AVWatch Started" Date() Time()

Log_Info = RXFInfo('.\CURRENT.LOG')

If Log_Info <> ''
   then do
        If SubStr(Log_Info,17,8) = Date('U')
           then do
                If Found('.\CURRENT.LOG','No virus found')
                   then If Found('.\CURRENT.LOG','Premature termination')
                           then Call AV_Interrupted
                           else nop
                   else Call No_No_Virus
                end
           else Call Not_Run_Today
        end
   else Call Log_Not_Found

Exit

Found: procedure
FileName = Arg(1)
String = Arg(2)
LineIn(FileName,1,0)
String_Found = 0
do while Lines(FileName) & \ String_Found
   FileLine = LineIn(FileName)
   If Pos(String,FileLine) > 0 then String_Found = 1
end
If String_Found then Return 1
                else Return 0
Return

Log_Not_Found: procedure
'GenAlert /T:"CURRENT.LOG not found. IBMAV did not run successfully."',
'/SEV:0 /TYPE:APPERR /APP:AVWATCH'
 Return

No_No_Virus: procedure
'GenAlert /T:"CURRENT.LOG lacks NO VIRUS FOUND message. Machine may be infected."',
'/SEV:0 /TYPE:APPWRN /APP:AVWATCH'
 Return

AV_Interrupted: procedure
'GenAlert /T:"IBMAV was interrupted on this machine."',
'/SEV:0 /TYPE:APPWRN /APP:AVWATCH'
 Return

Not_Run_Today: procedure
'GenAlert /T:"IBMAV not run in this machine today!"',
'/SEV:0 /TYPE:APPWRN /APP:AVWATCH'
 Return

Function_Error: procedure
'GenAlert /T:"AVWATCH ended with errors. Please check AVWATCH.LOG file."',
'/SEV:0 /TYPE:APPWRN /APP:AVWATCH'
 Exit
```

Figure 45. Sample AVWATCH.BAT Procedure to Check CURRENT.LOG Contents

Copy this procedure into the IBM AntiVirus directory of the machine to be monitored.

Go to the SystemView Manager to schedule the procedure. Under the SystemView Service Manager, start the Event Scheduler icon and select **New**.

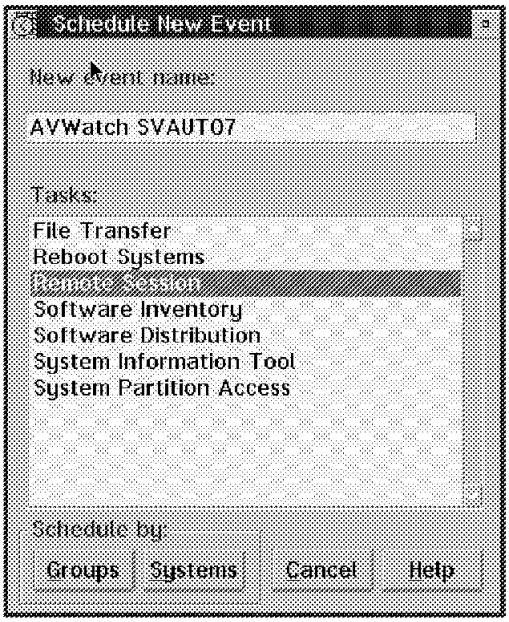


Figure 46. Schedule New Event Window

On the Schedule New Event window, type the name you would like this Scheduled Event to have in the New event name field (for example, AVWatch SVAUTO7).

Select **Remote Session** in the Tasks field and select **Systems** to select what workstation will be the target of this command. Choose **SVAUTO7** from the Systems list, and click on **Schedule**. You will be prompted to input the command to be issued in the target machine:

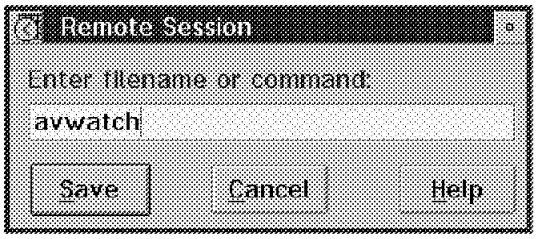


Figure 47. Input Remote Session Command

Type REXX AVWATCH.BAT and select **Save**. Now change the options on the Schedule Time and Date window.

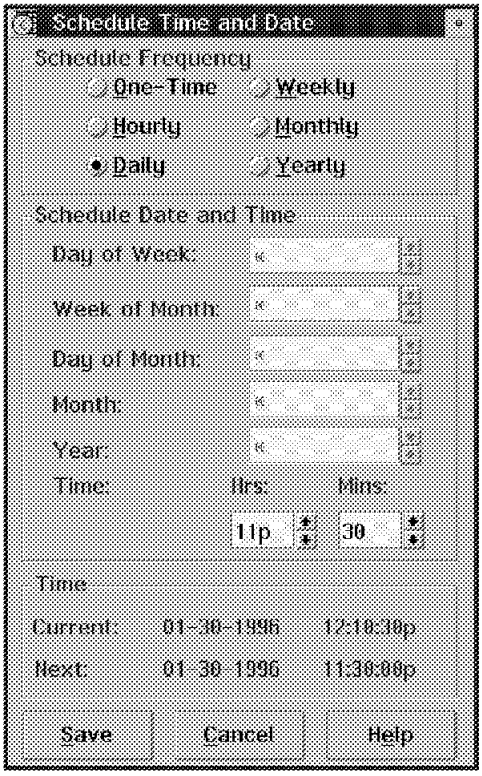


Figure 48. Schedule Time and Date Window

Choose the frequency AVWATCH, which should run according to how often IBM AntiVirus runs. In our scenario, we ran IBM AntiVirus daily, so we selected the **Daily** button under Schedule Frequency. This will make all fields unavailable under the Schedule Date and Time field, except for the Hrs and Mins fields. Choose a time late in the day to check for the IBM AntiVirus run (for example, 11:30 PM). Now select **Save** to save your schedule and exit the scheduler service.

2.3 NetWare Server Preparation

The software we used in this scenario on our NetWare 4.10 server was:

- NetFinity Services for NetWare
- IBM AntiVirus for NetWare

2.3.1 Install NetFinity Services for NetWare

NetFinity Services for NetWare may be installed from the NetWare console or from a NetWare Requester workstation. We installed it directly from the NetWare console.

If you are going to upgrade or re-install NetFinity, first make sure it is not running by issuing the following command at the console prompt:

```
UNLOAD NETFBASE
```

Otherwise, insert the NetFinity Services for NetWare disk 1 in your drive and start the install program with the following command:

```
LOAD A:\NETFINST
```

Follow the instructions on the screen. The install process will do the following:

- Ask you to input the target directory where you would like NetFinity to be installed
- Confirm the creation of the directory if it does not already exist
- Copy the necessary files
- Prompt you to change disks
- Prompt you to configure the Network Drivers
- Prompt you to choose whether to update AUTOEXEC.NCF

During the install, the Network Driver Configuration program is automatically started.

```
NetFinity Network Driver Configuration
 1: System Name : MANSERV1
 2: Network Drivers : Novell IPX
 3: Driver Enabled : True
 4: Keywords
    <Not Used>
    <Not Used>
    <Not Used>
    <Not Used>
    <Not Used>
    <Not Used>
    <Not Used>
    <Not Used>
 5: Network Time-Out : 15
 6: Options
 7: Save
 8: Reset
 9: Exit

Select an entry (1-9) -> _
```

Figure 49. NetFinity Network Driver Configuration Screen

Enter the name the SystemView Manager will use to identify this machine in option 1.

Use option 2 to select one of the available Network Drivers. To enable this driver, use value True in option 3. We have only enabled the IPX driver in this scenario, but it is possible to enable as many drivers as available. Please see the *IBM NetFinity Services for NetWare User's Guide* manual for details on enabling different drivers.

Enter any keywords used by the SystemView Manager to group workstations under option 4. Keep in mind that the keywords are case-sensitive. For example, svauto7 is not the same as SVAUTO7.

Use option 5 to set the Network Time-Out value. This determines how many seconds the SystemView Manager should wait for responses from this machine. If your network is very busy, you might want to increase this value.

Choose option 7 to save your configuration and option 9 to exit.

If you chose to update AUTOEXEC.NCF, the following statements will be added to automatically start NetFinity:

```
SEARCH ADD (NetFinity path)

LOAD NETFBASE
```

You have finished the NetFinity Services for NetWare installation.

2.3.2 Install IBM AntiVirus for NetWare

We used IBM AntiVirus for NetWare Beta Version 2.4c in this scenario.

IBM AntiVirus for NetWare can be installed by copying its files to any directory on a Novell NetWare server. We chose the SYS:\SYSTEM\IBMAVN, as recommended in the User's Guide installation procedure.

The following files were copied:

```
ENGFIX.DAT
IBMAVN.NLM    -- IBM AntiVirus NetWare start NLM
IBMAVN.PKG    -- Install status package file
IBMAVN3.NLM   -- IBM AntiVirus NetWare NLM for NW 3.1x with CLIB < 3.12F
IBMAVN3X.NLM  -- IBM AntiVirus NetWare NLM for NW 3.1x with CLIB >= 3.12F
IBMAVNW.NLM   -- IBM AntiVirus NetWare NLM for NW 4.x systems
READ.ME3      -- Notes and corrections on IBM AntiVirus NetWare's documentation
VIRSIG.LST    -- Virus Signature Data File
IBMAVN.PRF    -- IBM AntiVirus Profile settings for IBM AntiVirus NetWare
```

To start IBM AntiVirus for NetWare from the system console, enter the following:

```
LOAD SYS:\SYSTEM\IBMAVN\IBMAVN
```

The following screen will appear:

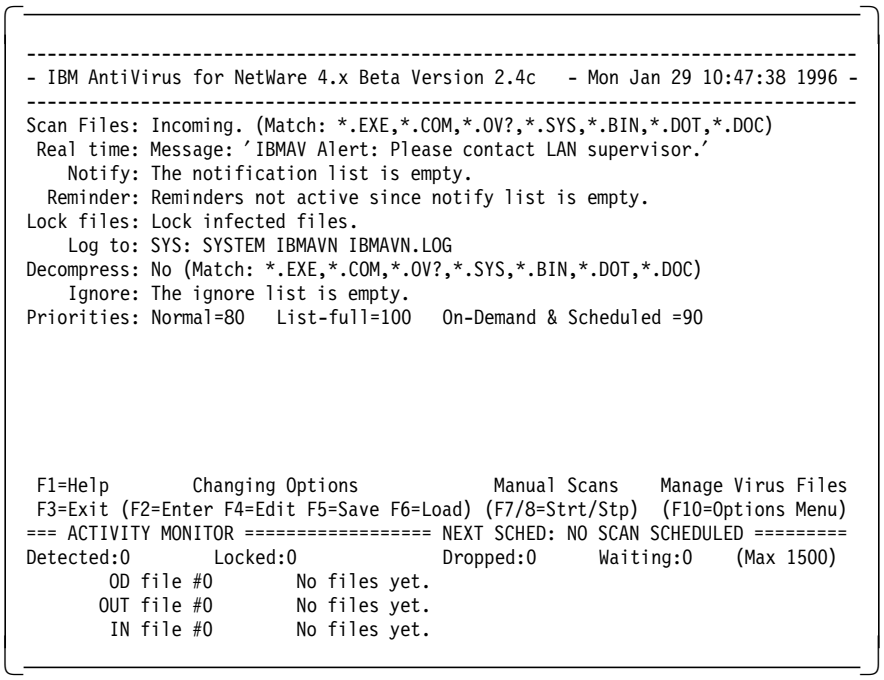


Figure 50. IBM AntiVirus for NetWare Console Screen

You have finished installing IBM AntiVirus for NetWare.

2.3.3 Customize MANSERV1 for the Automated Process

Steps to customize MANSERV1:

1. Set IBM AntiVirus parameters.
2. Set NetFinity Services to forward alerts to the SystemView Manager.
3. Set SystemView to monitor IBM AntiVirus execution.

2.3.3.1 Set IBM AntiVirus Parameters

Use the IBM AntiVirus for NetWare console to change IBM AntiVirus parameters. Press PF4 and the current settings will appear on a command line on the screen. Use the arrow keys to navigate through the command line (it is larger than the screen) and change the parameters you need.

Customize IBM AntiVirus in two ways in this automation scenario:

- To scan the NetWare server periodically
- Issue commands whenever it finishes scanning for viruses

The parameters -SCHED1, 2, 3, 4 and 5 specify when scheduled IBM AntiVirus scans will occur. Change one of them to the following format:

```
-SCHED1 DAILY 1996/01/30 17:00:00
```

This parameter setting will set IBM AntiVirus to daily scan the system at 5PM, starting on January 30, 1996.

The parameter -LOADNLM allows you to specify any NetWare executable to be run after a scan is completed whether or not a virus is found. Set the format of the -LOADNLM in the following way:

```
-LOADNLM VIRDETECT SYS:\SYSTEM\IBMAVN\NOTOK SCHED1 SYS:\SYSTEM\IBMAVN\OK
```

The LOADNLM parameter has two keywords: VIRDETECT and SCHEDn. After the VIRDETECT keyword, type the name of the NLM that will be executed in case a virus is found. After the SCHEDn keyword, type the name of the NLM that will be executed whenever SCHEDn is executed and no virus is found. Note that there may be as many SCHEDn keywords as actual schedules.

The NLMs specified in each keyword trigger GENALERTs with the following syntax:

OK.NLM:

```
GENALERT /T:"Successful Scan. No Virus Found" /APP:IBMAV /SEV:3 /TYPE:APPWRN
```

NOTOK.NLM:

```
GENALERT /T:"*** Virus Found Alert ***" /APP:IBMAV /SEV:0 /TYPE:APPWRN
```

These NLMs must be placed in the IBM AntiVirus directory.

There are many other parameters that can be set for IBM AntiVirus. If you need more detail on a specific parameter, please refer to the IBM AntVirus for NetWare User's Guide manual.

This completes the setting of IBM AntiVirus parameters in NetWare.

2.3.3.2 Forward Alerts to the SystemView Manager from NetFinity

All NetFinity Services for NetWare operation must be made from the SystemView Manager. To set NetFinity Services to forward alerts to the SystemView Manager, start the SystemView Manager GUI on your managing workstation. Double-click on the **Remote System Manager** icon and find MANSERV1 in one of the defined groups. Open the **MANSERV1** icon, and choose the **Alert Manager** option. This will display the Alert Log window as shown below:

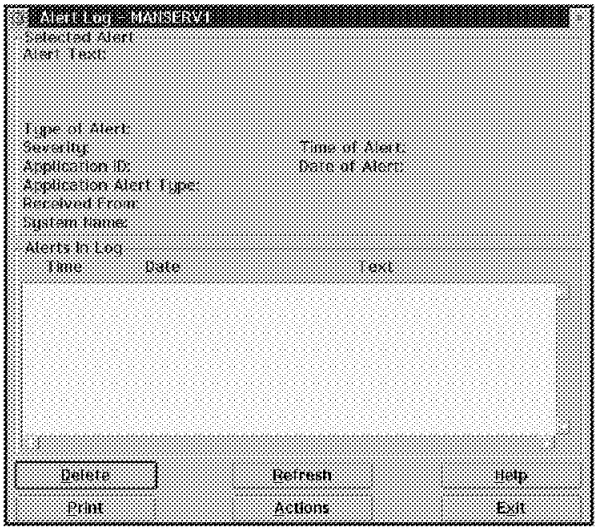


Figure 51. Alert Log Window for MANSERV1

The Alert Log window contains all alerts received by NetFinity from its own applications, alerts forwarded from other NetFinity/SystemView machines, and alerts generated by the GENALERT command.

Click on **Actions** to determine what actions NetFinity will take when our alerts arrive. In the Alert Actions window, click on **New**. This will display the Action Editor window.

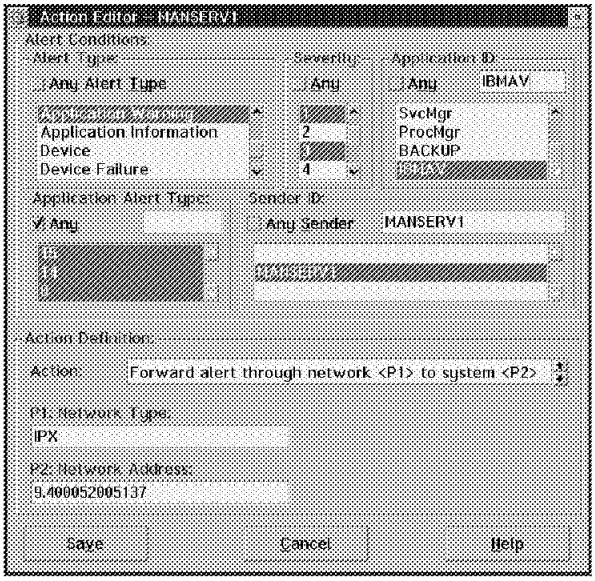


Figure 52. Alert Action Editor on MANSERV1

Specify under Alert Conditions what alert parameters will trigger the automated actions. As specified in 2.3.3.1, “Set IBM AntiVirus Parameters” on page 38, our Alert Type is Application Warning, the Severity is 0 or 3, and the Application ID is IBMAV. The Application Alert ID is not set, so highlight the **Any** check box. The Sender ID is our machine name, MANSERV1.

Under Action Definition specify what NetFinity will do when the above specified alert arrives. Search the Action field and click on the **Forward alert through network <P1> to system <P2>** option.

This will prompt you with two additional fields: P1: Network Type: and P2: Network Address:. Enter the network protocol, which NetFinity should use to send this alert, in the P1: Network Type: field. This network protocol must have been previously enabled in the NetFinity Driver Configuration (see Figure 49 on page 36) and must also be enabled on the SystemView Manager.

Enter the network address of the SystemView Manager in the P2: Network Address: field. This network address can be found in the SystemView Manager, under the Remote System Manager. Under All Systems, you will be able to get a Detail View of the workstations and check all of their protocols and addresses.

In our scenario, the Network Type is IPX, and our Network Address corresponding to the SystemView Manager is 9.400052005137. After you fill in the fields, select **Save** and confirm the new action created. This new action will be for both alerts when then occur. You will see the new action item that was just created appear in the Alert Actions window. You may exit the Alert Manager

now. You have finished setting NetFinity Services to forward alerts to the SystemView Manager.

2.3.3.3 Set SystemView to Monitor IBM AntiVirus Execution

We must make sure that IBM AntiVirus ran OK. After each successful run, we have customized IBM AntiVirus to issue a GENALERT indicating whether or not it has found a virus. We will need to check daily if that GENALERT was issued, so we know the virus scan actually happened.

What if IBM AntiVirus started and was abnormally interrupted without sending any genalerts? We will use the Process Manager and Error Conditions to handle that situation.

The Process Manager allows NetFinity to monitor all processes in a workstation. It informs you when a process runs, when it ends, and if it never started after the startup of the SystemView for OS/2.

Error Conditions are conditions that may be set to document specific error situations on a workstation. A workstation under an Error Condition has its icon overwritten with a red *circle and slash* in the SystemView Manager's Remote System Manager.

We will set an Error Condition of Virus Scan Started when IBM AntiVirus is started, using the Process Manager service. That error will get cleared by an alert issued with the -LOADNLM parameter. If IBM AntiVirus ends abruptly, the error condition will never be cleared and the Administrator can take the necessary actions.

Set the Process Manager to generate an alert when IBMAVN is run. This is done in the SystemView Manager under Remote System Manager. Make sure IBM AntiVirus is started on the NetWare Server. If it is not, you can do it using the Remote Session service. Double-click on **Process Manager** under MANSERV1. A list of all tasks will appear. Select IBMAVN task's context menu by clicking once with the right mouse button on it, then select **Add process alert...**, as shown in Figure 53.

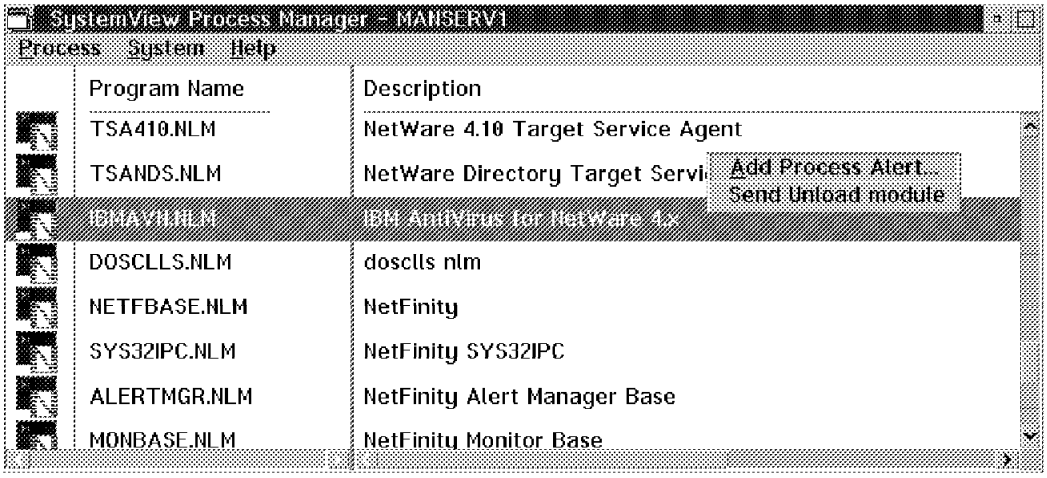


Figure 53. Process Manager for MANSERV1

The Add Process Alert window will appear.

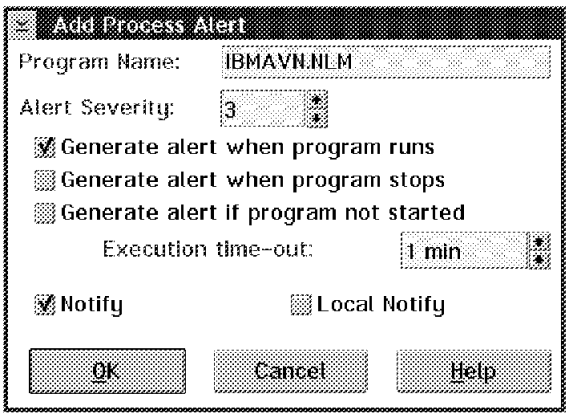


Figure 54. Add Process Alert Window

Highlight the **Generate alert when program runs** check box, so that the Process Manager will issue an alert every time IBMAVN is started. Set the Alert Severity to 3, and highlight the **Notify** check box so the alerts are sent to this manager workstation. After you make these changes, select **OK**. The Process Manager alert has been created. If IBMAVN.NLM is running, you will immediately receive an alert. You may close all MANSERV1-related windows now.

With all of the alerts coming to the SystemView Manager, it is now time to customize it to set an Error Condition for the Process Manager Alert, and to clear the Error Condition for the -LOADNLM alerts. Go to the Alert Manager and select **Actions**, then **New**. In the Action Editor, set the Alert Conditions Alert Type to Application Information, the Severity to 3, the Application ID to ProcMgr, the Application Alert Type to Any and the Sender ID to your NetWare Server's address. Our NetWare Server's address was IPX::30AA0F92.000000000001. Select **Set error condition '<P1>' for sending system** under Action Definition. Enter the Error condition type in the P1: Error condition field. The Error Condition type should be Virus Scan Started. Select **Save** to save this new action.

Now add the action to clear the Error Condition. Select **New** again, and in the Action Editor, set the following Alert Conditions:

- **Alert Type** to Application Warning
- **Severity** to 3 or 0
- **Application ID** to IBMAV
- **Application Alert Type** to Any
- **Sender ID** to your NetWare Server's address

Select **Clear error condition '<P1>' for sending system** under Action Definition. Input the Error condition type in the P1: Error condition field. The Error Condition type should be Virus Scan Started. Make sure you spell Virus Scan Started correctly. It must match the string input in the Set Error condition action we set before to actually clear the Error condition. Select **Save** to save this new action.

We want this Virus Scan Started condition cleared, but if it was cleared by a Virus Found alert, then we want another Error condition set to document the virus presence. Virus found error conditions should only be cleared manually by the administrator.

Repeat the steps to create an action to set an Error Condition when a Virus Found alert is received. You should have the following alert conditions set in the Action Editor:

- **Alert Type** to Application Warning
- **Severity** to 0 when a virus is found
- **Application ID** to IBMAV
- **Application Alert Type** to Any
- **Sender ID** to Any

This setup will cause Error Conditions to be set whenever a virus is detected in any of the monitored systems.

2.4 OS/2 Warp Connect Client Preparation

The OS/2 Warp workstation has IBM AntiVirus for OS/2, SystemView Services for OS/2 and ADSM OS/2 Client already installed. We will customize it for the automated process in the following way:

- Set IBM AntiVirus to run periodically.
- Set IBM AntiVirus to issue an alert when a virus is found.
- Set NetFinity Services to forward alerts to the SystemView Manager.
- Schedule SystemView to check if IBM AntiVirus has run.

The OS/2 Client customization for the above steps is the same as the Windows 95 Client customization. Please perform the steps described in 2.2.4.1, “Set IBM AntiVirus to Run Periodically” on page 27 through 2.2.4.4, “Schedule SystemView to Check IBM AntiVirus” on page 32, replacing any reference to the Windows 95 workstation SVAUTO7 with the OS/2 Client workstation SVAUTO0.

In 2.2.4.4, “Schedule SystemView to Check IBM AntiVirus” on page 32, use the AVWATCH.CMD below instead of AVWATCH.BAT. OS/2 has the advantage of supporting REXX command files which are a lot more flexible than any .BAT file.

```
/* REXX */
Trace off
Call RxFuncAdd 'SysLoadFuncs', 'RexxUtil', 'SysLoadFuncs'
Call SysLoadFuncs
Say "AVWatch Started" Date() Time()

If SysFileTree('.\CURRENT.LOG','found_file','FT') <> 0
   then Call Function_Error

If found_file.0 > 0
   then do
        If SubStr(found_file.1,1,8) = Date('O')
           then do
                If SysFileSearch('No virus found.','.\CURRENT.LOG','No_Virus.') <> 0
                   then Call Function_Error
                If No_Virus.0 = 0
                   then Call No_No_Virus
                   else do
                        If SysFileSearch('Premature termination','.\CURRENT.LOG','Terminated.') <> 0
                           then Call Function_Error
                        If Terminated.0 > 0
                           then Call AV_Interrupted
                        end
                end
           else Call Not_Run_Today
        end
   else Call Log_Not_Found

Exit

Log_Not_Found: procedure
'GenAlert /T:"CURRENT.LOG not found. IBMAV did not run successfully." /SEV:0 /TYPE:APPERR /APP:AVWATCH'
 Return

No_No_Virus: procedure
'GenAlert /T:"CURRENT.LOG lacks NO VIRUS FOUND message. Machine may be infected." /SEV:0 /TYPE:APPWRN
/APP:AVWATCH'
 Return

AV_Interrupted: procedure
'GenAlert /T:"IBMAV was interrupted on this machine." /SEV:0 /TYPE:APPWRN /APP:AVWATCH'
 Return

Not_Run_Today: procedure
'GenAlert /T:"IBMAV not run in this machine today!" /SEV:0 /TYPE:APPWRN /APP:AVWATCH'
 Return

Function_Error: procedure
'GenAlert /T:"AVWATCH ended with errors. Please check AVWATCH.LOG file." /SEV:0 /TYPE:APPWRN /APP:AVWATCH'
 Exit
```

Figure 55. Sample AVWATCH.CMD Procedure to Check CURRENT.LOG Contents

No further customization is necessary for the OS/2 Workstation.

2.5 DOS/Windows Client Preparation

Follow the same steps taken to customize the Windows 95 client. Replace any references to the Window 95 client name SVAUTO7 and addresses with the DOS/Windows client name SVAUTO8 and respective addresses.

Chapter 3. Automating ADSM/2 Using SystemView/2

This chapter shows the integration and automation of ADSM into SystemView for OS/2, and it includes the following topics:

1. Restoring a file once it has been changed
2. Restore and back up operations generating alerts
3. Scheduling a back up and building a genalert

The three environments we have worked with will be covered in the following order:

- OS/2 using NetBIOS
- NetWare using IPX/SPX
- Windows 95 using TCP/IP

3.1 ADSM Client for OS/2

This sample works with the following SystemView for OS/2 services:

- Critical File Monitor
- Alert Manager

  Also, it will integrate into the sample:

- ADSM server and client

The intent is to show you how to configure SystemView for OS/2 to use the automatic restore process of ADSM.

3.1.1 Critical File Monitor

Using the Remote System Manager of SystemView for OS/2, you can access the Critical File Monitor service. Instead of using the default files that are in the monitor list for the Critical File Monitor, we can add additional files by double-clicking on the field for **Additional Monitored Files**. Then we can either enter the file name or use the mouse to scroll down the path to the correct file. An example of this is shown in Figure 56.

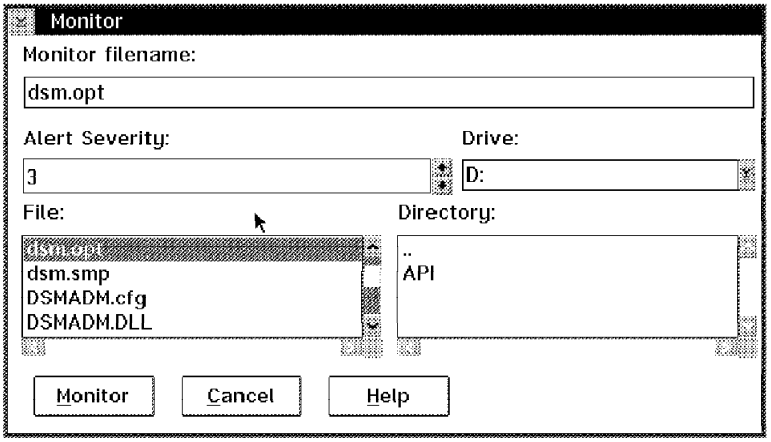


Figure 56. Critical File Monitor

3.1.2 Alert Manager

The next service that you will use in this example is the Alert Manager. To start using the Alert Manager, just click on the Alert Manager icon in the Service Manager window for the remotely controlled system.

After clicking on Actions and New, you will get a window similar to Figure 57. The default window that comes up will have many of the defaults checked off to filter on *All*. of the actions in the sub category. In order to better match the criteria for the alert action, you should select the specific values instead of saying any value in the Action Editor.

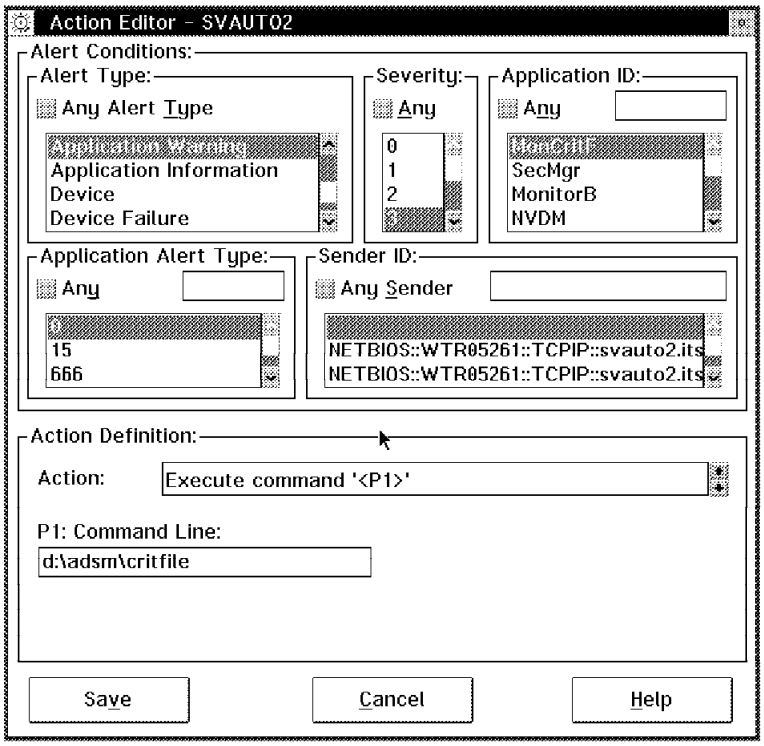


Figure 57. Action Editor

The fields we configured are as follows:

- Alert type of **Warning**.
- Severity equal to the value you selected in the Critical File Monitor.
- Application ID of MonCritF.
- Application Alert Type needs to match what you see in the alert record. Note that the value must match exactly. A value of 0000 does not equal 0.
- Sender ID to match this system. In this case, it would mean selecting the blank line.
- Action value of Execute command '<P1>'.
- P1:command Line: will be the executable that we wish to run, `d:\adsm\critfile`

After saving this alert filter, change the action field to save a copy of this alert to the log, so that you can see it later on. This will result in you having two separate filters set up for the same alert.

3.1.3 ADSM

If you are not familiar with using and starting ADSM, the following section will show you:

1. Installation of ADSM
2. Setup
3. Additional definitions

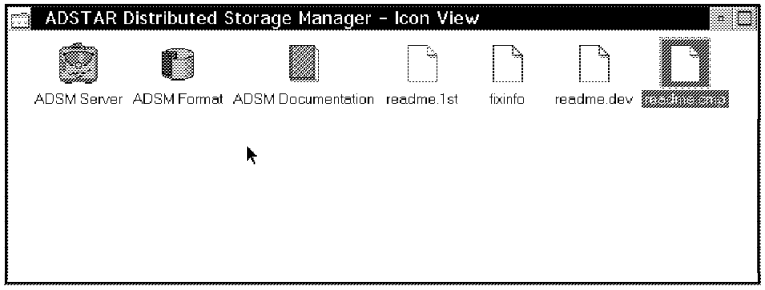


Figure 58. ADSM Server Icons

3.1.3.1 Installation

The installation of ADSM server is quite simple. You will only have to follow the sequence of diskettes. Figure 58 and Figure 59 show the icons for the ADSM server and the icons for the ADSM client after it has been installed.

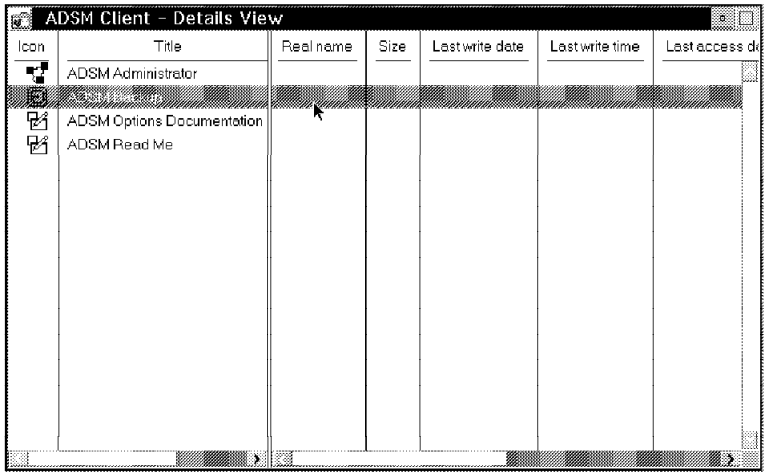


Figure 59. ADSM Client Icons

3.1.3.2 Setup of ADSM

This process is a little more complex and includes:

- Editing options files for the server and client
- Allocation and formatting disk storage pools
- Registering the administrators user ID

Editing the options file is very similar for the server and the client. In either case you can use the SAMPLE.OPT file that comes with the code. You may decide to modify it for your own environment or use it as is. This option file is used to customize the following:

- Communication protocols
- Number of client licenses
- Passwords
- Include and exclude list

Figure 60 shows the DSMSRV.OPT file that is associated with the server we used. We used NetBIOS and TCP/IP. If you are using TCP/IP, you will need to know the servers address. If you use NetBIOS you will need to know its NetBIOS workstation name. The NetBIOS name can be found in the IBMLAN\IBMLAN.INI file.

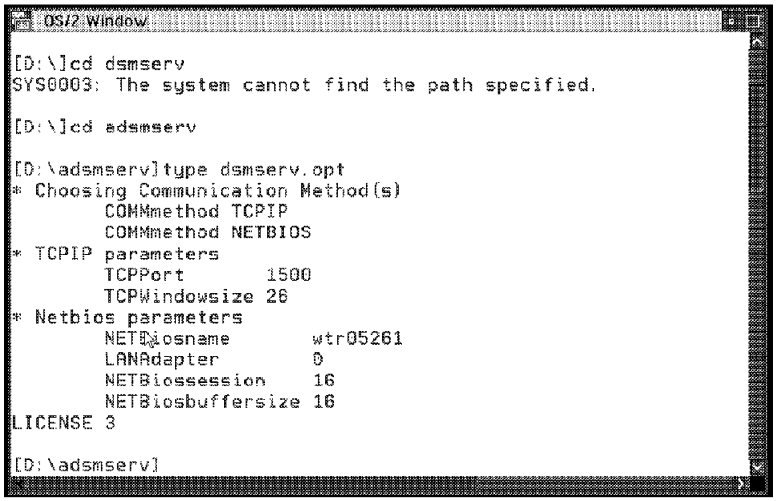


Figure 60. ADSMSRV.OPT File

You can either manually update the options file for the number of licenses, or you can update the number with the following command:

* REGISTER LICENSE #

This will add the statement to the DSMSRV.OPT file for you.

Once you have created the options files (Server and Client) you will have to register some user IDs. This and almost everything can be done through the GUI that runs on the client or through the command line. If you decide to use the command line the command is:

* REGISTER ADMIN USERID PASSWORD=XXXXXXX

Adding the EXCLUDE/INCLUDE list is one of the most important points. This sets up which files are not going to be backed up even if a selective command is executed.

The construction of this list requires you to do some planning. You will need to be careful of the order of the statements. ADSM processes the options file from the bottom up so if you enter the statements in the following order:

- * INCLUDE c:\ADSM\DSM.opt
- * EXCLUDE c:\ADSM*

ADSM will first check the last sentence, the EXCLUDE one. When it gets to the next line, it will get thrown away because it has already done the exclusion. If the sentences are placed in the reverse order, then from the ADSM directory, all files except DSM.OPT will be backed up:

- * EXCLUDE c:\ADSM*
- * INCLUDE c:\ADSM\DSM.OPT

Part of the setup process is to prepare the place where you are going to put the backups and archives. You will have to format that space before it can be used for backup purposes. The command to set up this backup area and format is as follows:

```
* DSMFMT {-k|-m} {-db|-log|-data} {filename) (size1)
```

An actual example would be: `* DSMFMT -m -data SVAUTO02 10`

3.1.4 Additional Definitions

The additional definitions for setting up ADSM are:

- Define Storage Pools
- Define Volumes
- Define Domain
- Define PolicySet
- Define Mgmtclass
- Define Copygroup
- Assign Defmgmtclass
- Validate Policyset
- Initialize Policyset
- Define Nodes

All these steps are needed in order to be able to make backups and restores.

You might find it easier to define all of the process through the GUI. If you prefer using the command line, following are some useful examples of syntax:

- Define StgPool LEO_FRO DISK ACCESS=READWRITE

  This statement will allow you to create a volume which will contain one or more formatted spaces. This can make administration easier.

- Define Volumes SVAUTO02 LEO_FRO DISK ACCESS READWRITE

  This statement will link the formatted space with a specific volume. In this case, SVAUTO02 will be part of volume LEO_FRO.

- Define domain SVAUTO DESCRIPTION=″DOMAIN FOR SYSTEMVIEW″

  This domain contains all of the required definitions to store data, and the administration of the system. It allows the creation of a tree structure where you can have many policies set up for different classes.

- Define PolicySet SVAUTO RULES DESCRIPTION=″RULES FOR SYSTEMVIEW″
- Define Mgmtclass SVAUTO RULES CLASS DESCRIPTION=″CLASS FOR SV″
- Define Copygroup SVAUTO RULES CLASS STANDARD TYPE=BACKUP DESTINATION=SVAUTO02

  This is very important as it defines in which volume you are going to put the information and if this information is from a backup or from archives.
- Assign Defmgmtclass SVAUTO RULES CLASS

  The default class for domain SVAUTO will be CLASS.
- Validate Policy set SVAUTO RULES
- Activate Policy set SVAUTO RULES
- Register Node NODE1 XXXXX Domain=SVAUTO

  This is the registration of a node called NODE1 with domain SVAUTO and password XXXXX. If this node executes a backup operation the information will be stored in: SVAUTO-RULES-CLASS-LEO_FRO-SVAUTO02.

These are the main statements which will enable you to execute backups successfully. This is the hard way to get ADSM to work. It is much easier to set it all up using the GUI. Figure 61 shows the key icons that are used in the setup:

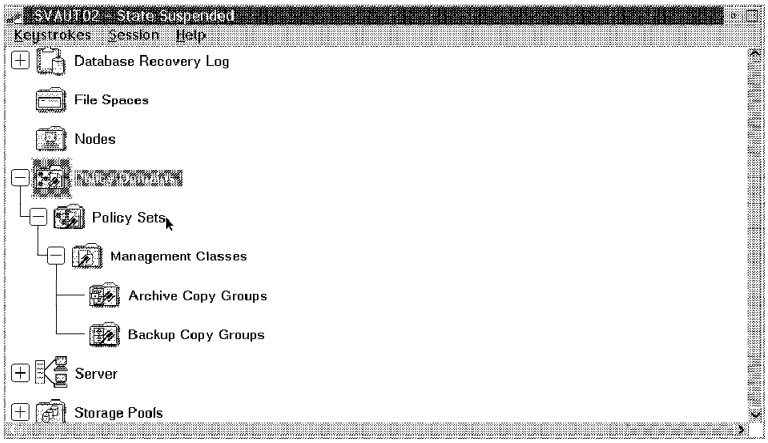


Figure 61. ADSM Policy Set

3.1.4.1 Sample 1 Restoring a File Once Its Been Changed

We created a very simple REXX EXEC that will help you see what is going on during the process. The EXEC appears in Figure 62 on page 51.

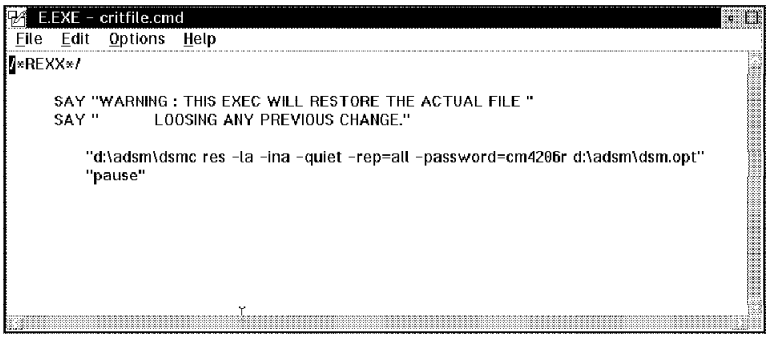


Figure 62. REXX Program CritFile.CMD

The command here is:

```
d:\adsm\dsmc res -la -ina -quiet -rep=all -password=cm4206r
d:\adsm\dsm.opt
```

This command contains some options that are explained below:

- LAtest - It restores the most recent backup version of the file.
- INActive - Specifies that you want ADSM to display both active and inactive versions of files.
- Quiet - Prevents messages from being displayed on your screen during processing.
- REPlace - This option shows which files can be overwritten. In our case, this option will allow replacement of the changed file with the original version.

It is very important to indicate the file that you want restored. In this example we selected the file dsm.opt. Before testing this scenario, we needed to verify a few things. First, we needed to verify whether the file that was going to be recovered had been backed up. Secondly, we need to verify whether the file dsm.opt was modified, by adding the statement INCLUDE path/filename. This prevented problems from occurring. Figure 63 on page 52 shows our dsm.opt file.

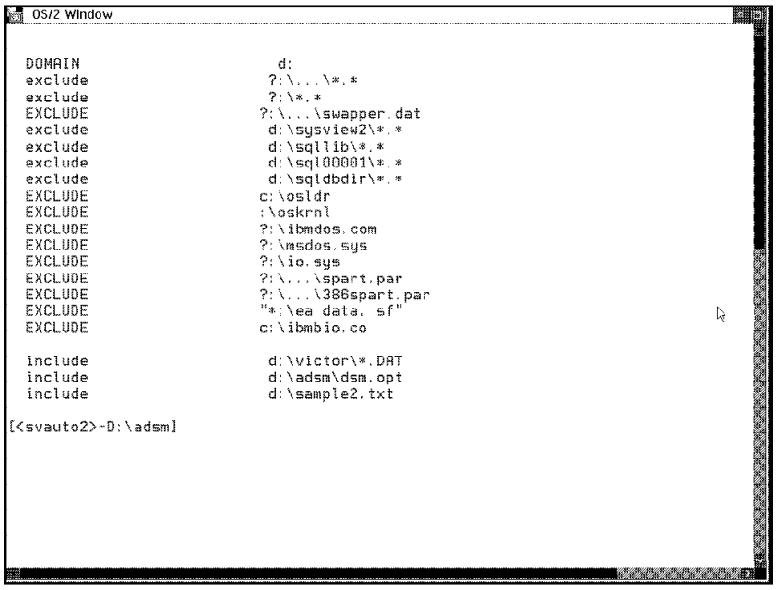


Figure 63. DSM.OPT File

The syntax used to back up a file is as follows: `d:\adsm\dsmc selective -password=xxxx path:\filename`. Once you have done all of the above steps and the setup for ADSM, the environment will be ready to operate. Let's modify the file you have selected.

Soon after modifying the file, your machine will send an alert to the log, as you can see in Figure 64.

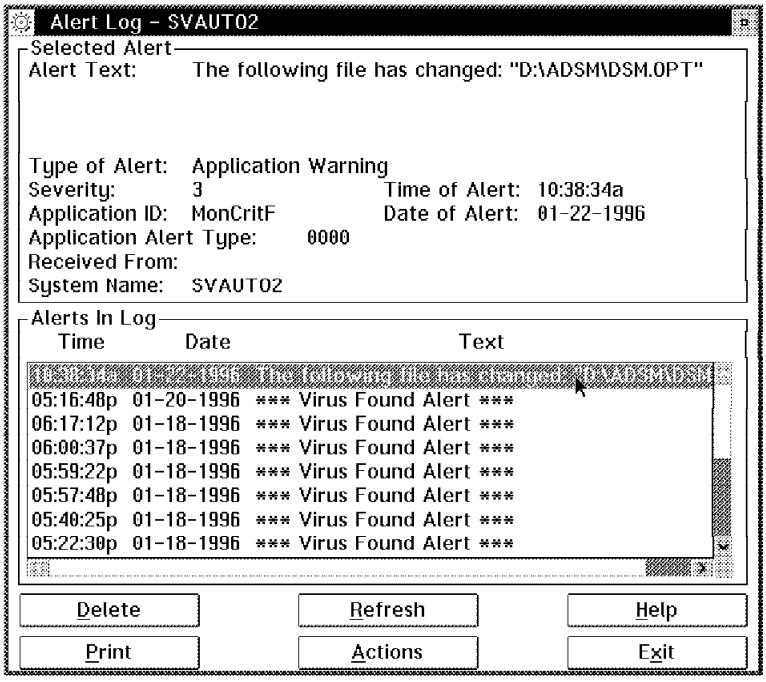


Figure 64. Alert Log

If you select the latest alert and Actions you will see the alert that was generated. As a result of the alert, an automatic process was kicked off to restore the file. The process output *CRITFILE.CMD*, is shown in Figure 65 on page 53.

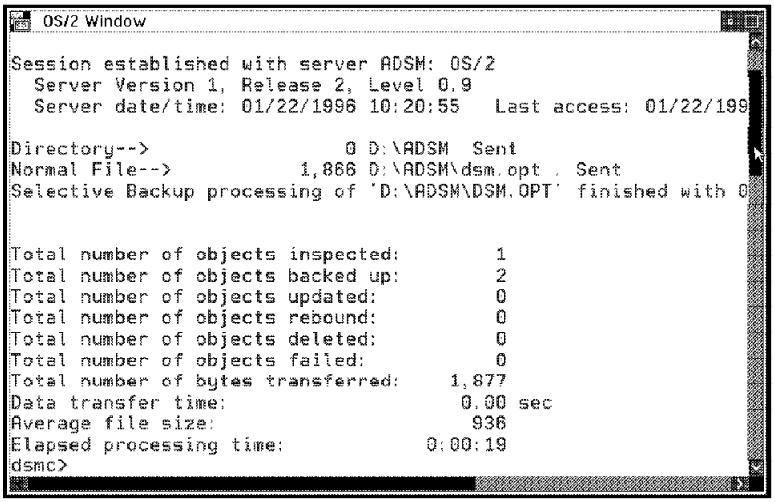


Figure 65. Restoration Process

3.1.4.2 Sample 2 Backup/Restore Using Alerts

This scenario will show you how to integrate ADSM using some *genalerts* and a simple REXX program. The program will take, as input, the names of the files you wish to back up or have restored and use genalerts to drive the process. Our simple REXX example can be seen in Figure 66 on page 54. The statements in the EXEC are as follows:

- ″GENALERT /T:″||msg||″/APP:BACKUP /SEV:2 /TYPE:SECWRN /ATYPE:310″
- ″d:\adsm\dsmc selective -password=xxxx ″||fn

Where in the first command:

- MSG - String containing a message with the name of file or files to be backed up. The name is the fn variable as shown in Figure 66 on page 54.
- APP - Is the name of the generic alert and could be anything.
- SEV - Indicates the severity you are assigning.
- TYPE - It must comply with the SystemView standards.
- ATYPE - It could be any number, but it must be unique.

In the second command we have the following:

- dsmc - This is the command to start a session using the command line in the ADSM client.
- selective - Is an option of dsmc that allows you to make a back up indicating the path of the file you want to have backed up. The file name in this case ends with *fn* (we are concatenating all the sentence with the value fn).
- password - This is the password you assigned to your ADSM node when it was registered with the server.

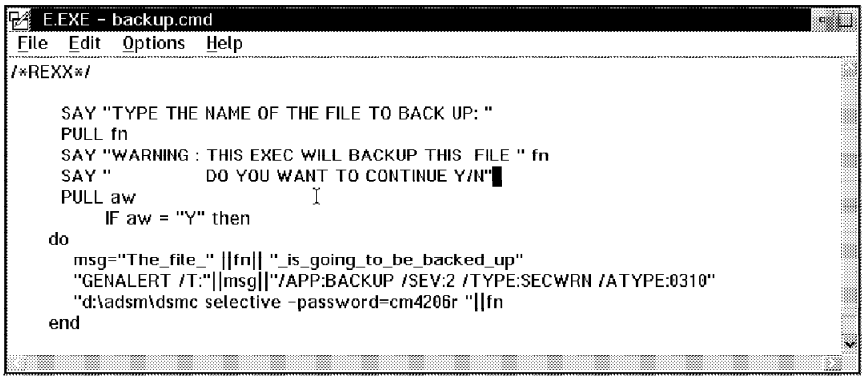


Figure 66. BACKUP.CMD File

Once you have edited the program, you will open an OS/2 window and execute the program `d:\adsm\backup.cmd`. You should also check to be sure that the server is started.

The result of issuing the command should look like the following screen:

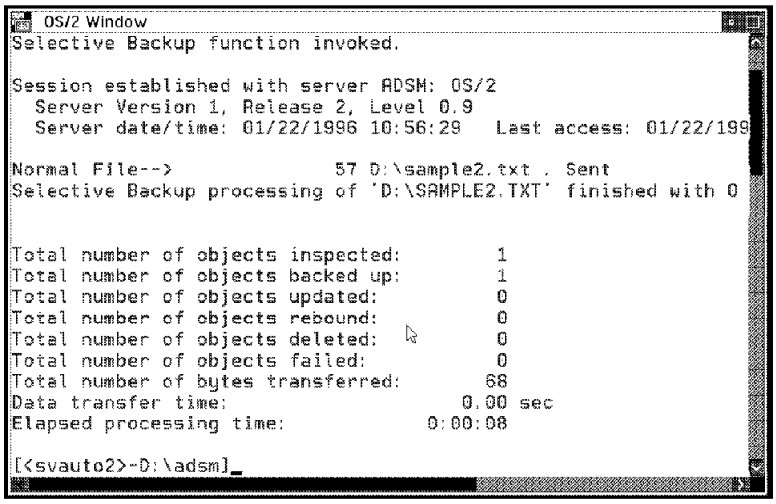


Figure 67. BACKUP.CMD Execution

A result of issuing the EXEC is to create an alert. The following figure shows you the alert log.

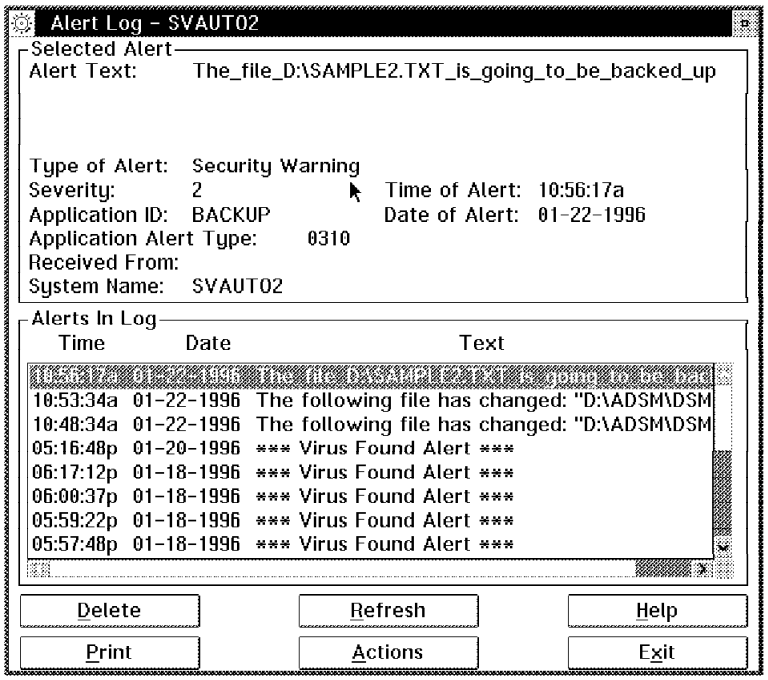


Figure 68. Alert Log for BACKUP Command

The process for restoring files is almost the same. Figure 69 show what the restore EXEC looks like. An explanation of the commands used in the EXEC follows:

- "GENALERT /T:"||msg||"/APP:RESTORE /SEV:2 /TYPE:SECWRN /ATYPE:300"
- d:\adsm\dsmc res -la -ina -quit -rep=all -password=xxx"||fn

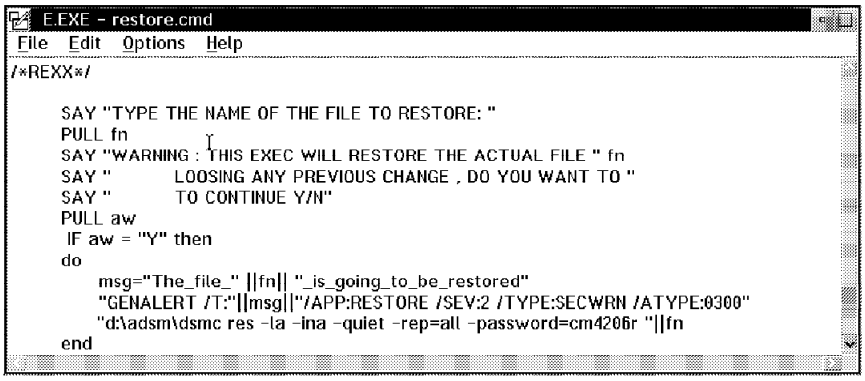


Figure 69. RESTORE.CMD File

The next step to show the implementation of the EXEC is to delete the file you backed up and run the restore command.

It should look like Figure 70 on page 56.

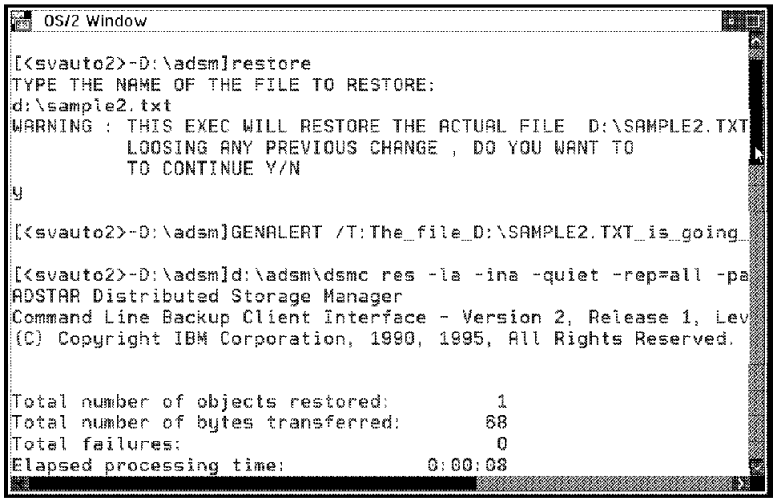


Figure 70. RESTORE.CMD Execution

As we saw with the backup command, the generic alert will let you keep track of what actions have taken place. When you get the alert it should look like Figure 71.

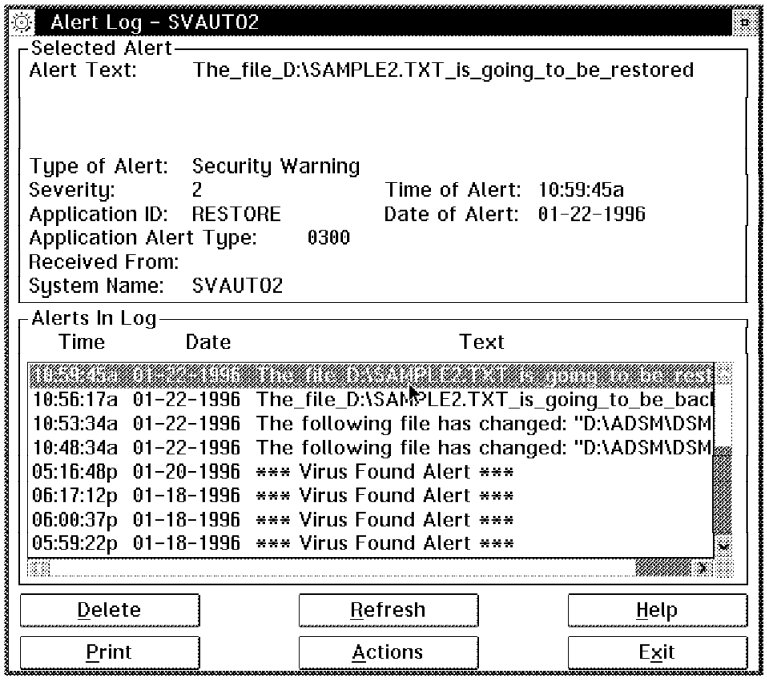


Figure 71. Alert Log for RESTORE Command

3.1.4.3 Sample 3 Scheduling Back Up Operations

This section shows the integration of the first two samples. A REXX program was written to provide the following:

- Generic Alert
- User interface
- Alert Log

As you can see in Figure 72 on page 57 and Figure 73 on page 57, there are other interesting commands that we will take a look at.

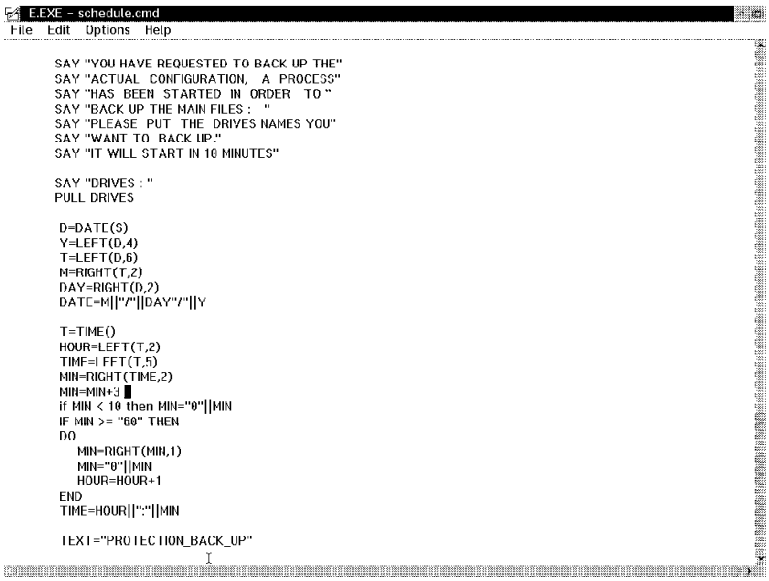


Figure 72. SCHEDULE.CMD File

The first part of the EXEC only deals with formatting the time and the date. We will skip that for now and review the bottom section in the EXEC.

Figure 73. SCHEDULE.CMD File Second Part

1. ″d:\adsm\dsmadmc -id=xxxxx -pa=xxxxx define schedule svauto adsm desc=″||text″ act=selective object=″||drives|| ″ priority=1 startd=″||date|| ″startt=″||time||″ dur=2 duru=minutes per=1 peru=days day=any″

2. ″d:\adsm\dsmadmc -id=xxxxx -pa=xxxxx define association svauto adsm LEO_FRO″
3. ″genalert /t:″schedule_backup_on_going″ /app:schedule /sev:3 /type:sysflt /atype:320″
4. ″d:\adsm\dsmc sched -queryschedperiod=1 -retryperiod=1 -password=xx″

The first sentence is made up of two commands. The first one gives you a session from the client to the ADSM server. As we already saw, the userid and password are created at the server using a command or a graphical interface in the client. The second part is a little more complex. It deals with the scheduling option that will allow you to program a backup operation. The options on this command are as follows:

- SVAUTO - This is the name of the domain.
- ADSM - This is the name of the schedule.
- ACT = Selective - This mode allows you to create a backup.
- Object = Drives - This is the name of the variable who contains the path and file or files to be backed up.
- Priority = 1 - Means the priority that ADSM is going to use to process the request. The highest priority is 1.
- Startd - Indicates the start date. It should be in the format MM/DD/YYYY.
- Startt - Indicates the start time. It should be in the format hh:mm.
- Dur = 2 is the time window in which ADSM will start the backup.
- Duru = Minutes is the units used for the duration.
- Per - Indicates when it is going to be repeated.

2) The next command is very important because it defines the relationship between the schedule we already created and the receiving node.

- SVAUTO - This is the name of the domain.
- ADSM - The is the name of the schedule.
- LEO_FRO - This is the node name that is going to receive the back up action.

The last command is the most important, without this command the backup will not start. This command allows the client to wait for scheduled events on the server.

- DSMC - This is the client command mode.
- QUERYSCHEDPERIOD = 1 - This means that every hour it will look for new events.
- RETRYPERIOD = 1 - This means that if the operation fails, it will try again in a minute.
- Password - This is the password you set up when you registered.

Once you run this EXEC, you will get something like Figure 74 on page 59.

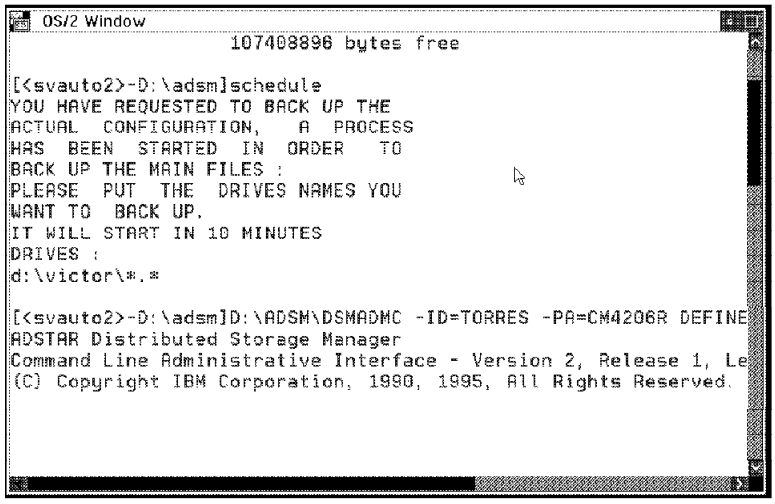


Figure 74. SCHEDULE.CMD Execution

As you can see, these commands are executed in a batch interactive form. You will get prompted to enter the file names that you want to include in the scheduled backup. As soon as you press enter, you will see the Alert log, indicating the transaction has been scheduled. While you wouldn't normally have sent the alert in a way to cause it to pop up on the monitor, we did so to show you the process flow.

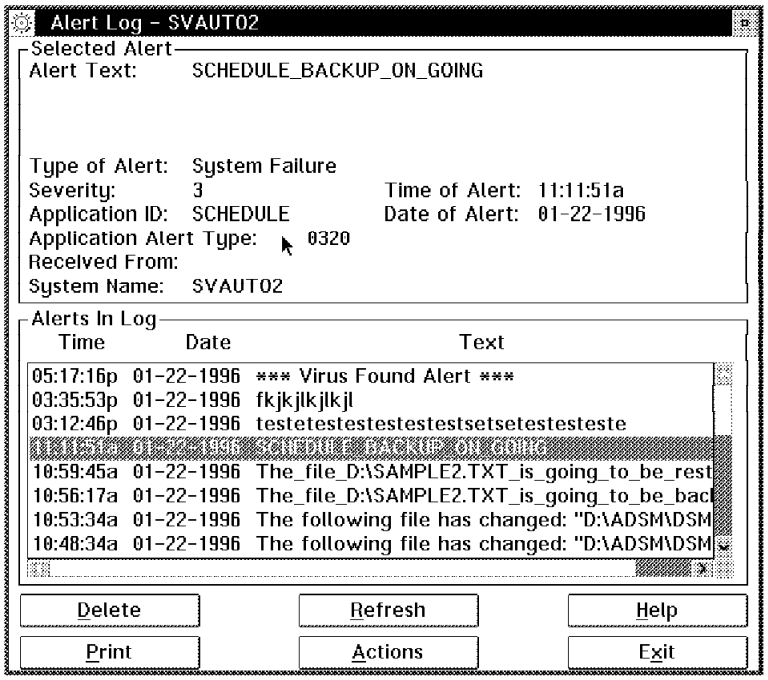


Figure 75. Alert Log for SCHEDULE Command

If you check Figure 75, you will see that the contents of the alert matches the option values you added in the EXEC.

Finally, Figure 76 on page 60 and Figure 77 on page 60 show the execution flow.

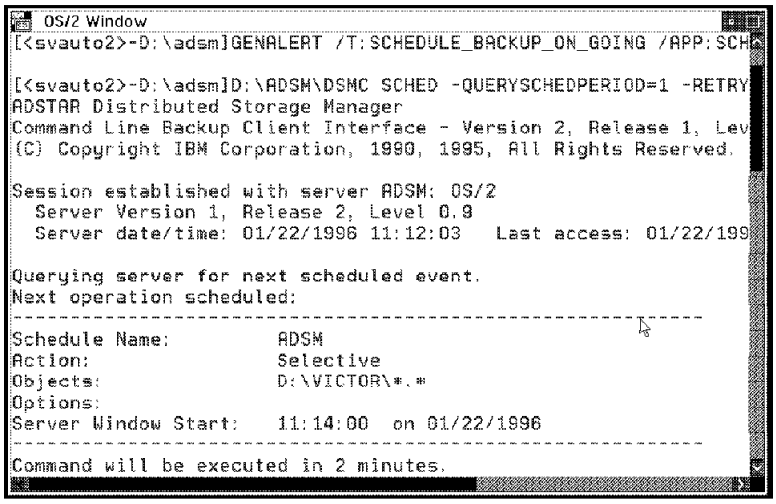


Figure 76. SCHEDULE.CMD Execution

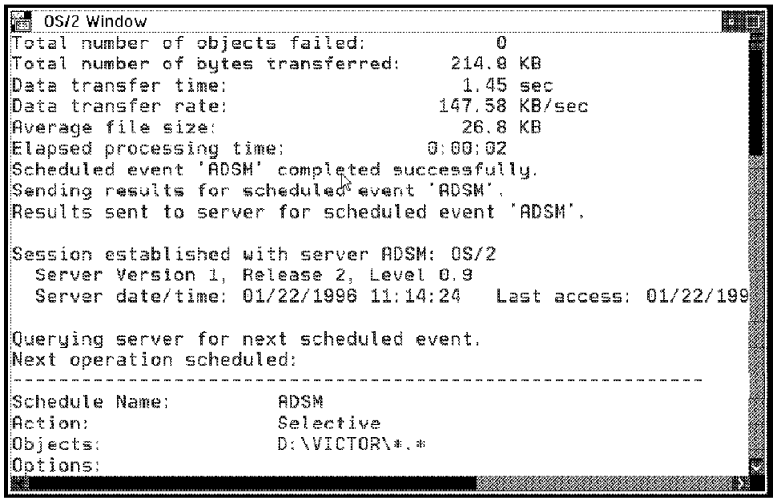


Figure 77. SCHEDULE.CMD Execution

3.2 ADSM Client for Windows 95

This example deals with the following:

- Critical File Monitor
- Alert Manager
- ADSM client for Windows 95

The purpose of this section is to show you how to integrate ADSM and SystemView for OS/2 together when the client is a Windows 95 system.

3.2.1 Critical File Monitor

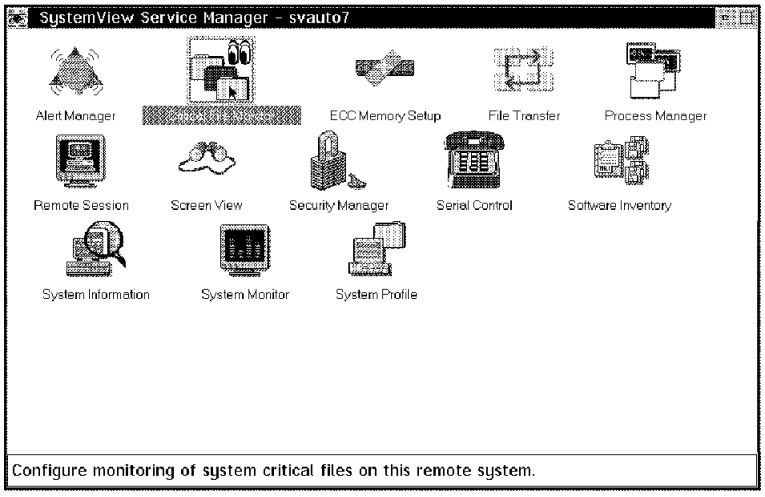


Figure 78. Services Manager

The process for monitoring a file under Windows 95 using the Critical File Monitor is exactly the same as what was done under OS/2. Adding a new file to be monitored will let you know if a change has occurred on a monitored file, and can result in the automatic restoration of a file using ADSM.

As you can see in Figure 79, when you add the new file to be monitored, it asks you for a severity. This information will be sent to the alert manager when the alert flows. By default, the alert contains information about the alert type, application ID, application alert type and information about who is sending the alert. The function of the alert management process, in this case, would be to automatically execute an ADSM command if the alert passes through a filter.

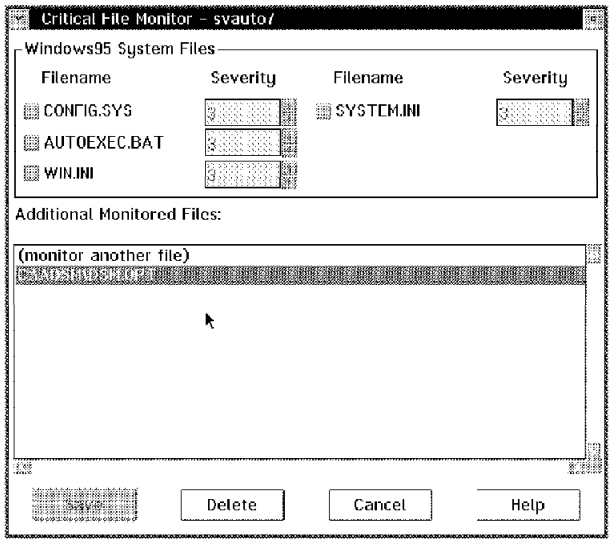


Figure 79. Critical File Monitor

3.2.2 Alert Manager

In Figure 80 you can see the options that were customized within the alert manager for our scenario. One of the fields is the Action Definition field. We set this field to this sample we will use Execute Command <P1>, and the following field to the ADSM command that we will execute. In this case, it is the restore command.

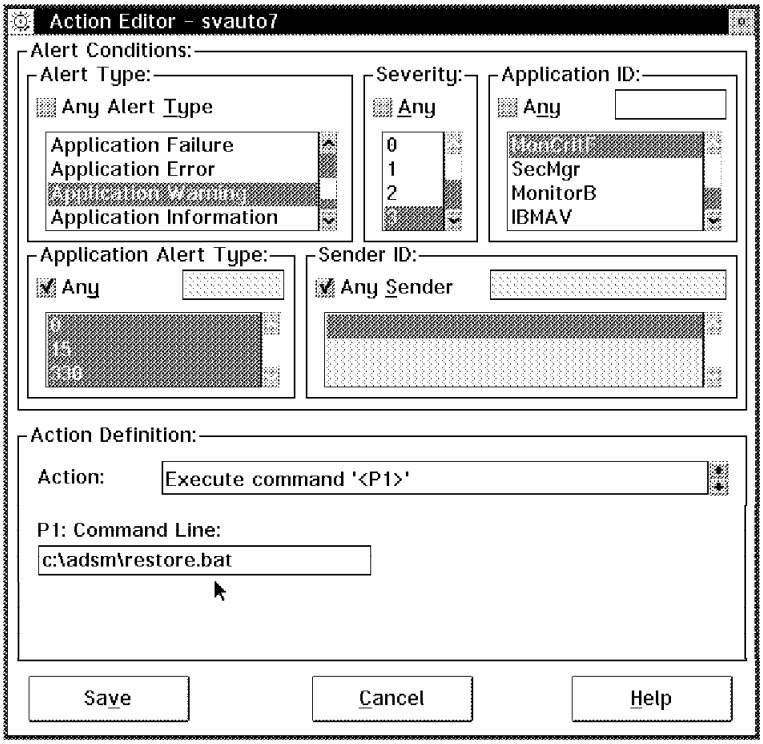


Figure 80. Action Editor

3.2.3 ADSM Client for Windows 95

The things that we will be concerned with in this part of the sample are:

- The options file DSM.OPT
- The communications protocol being used
- The files that will be excluded from the backup
- The ADSM domain name and the node name

Make sure that the file extension is BAT instead of CMD.

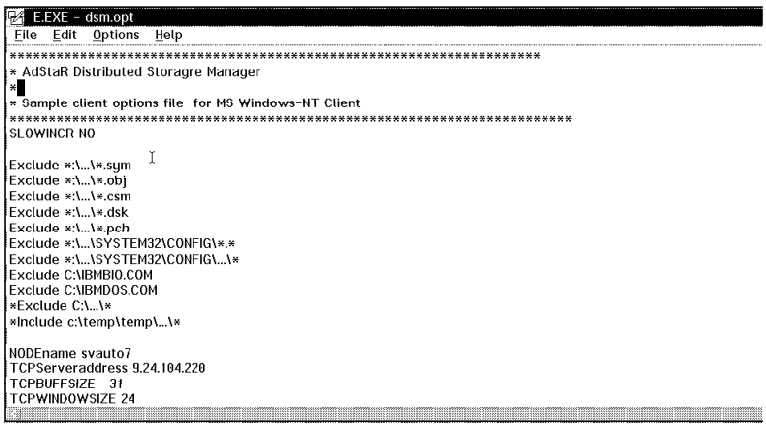


Figure 81. DSM.OPT File

3.2.4 SAMPLE 1 Restoring a File Once It Has Changed

This sample is just like the one we created in the OS/2 scenario; the only differences being the file name extension and some ADSM command options. The BAT file is shown in Figure 82. When the file DSM.OPT is changed, an alert will flow, and it will show up in the alert log, as shown in Figure 83 on page 64.

Figure 82. RESTORE.BAT Program

As you can see in Figure 83 on page 64, the alert comes to the log; if you want to display it in a pop-up window, then no matter what you are doing, it will show up the new alert.

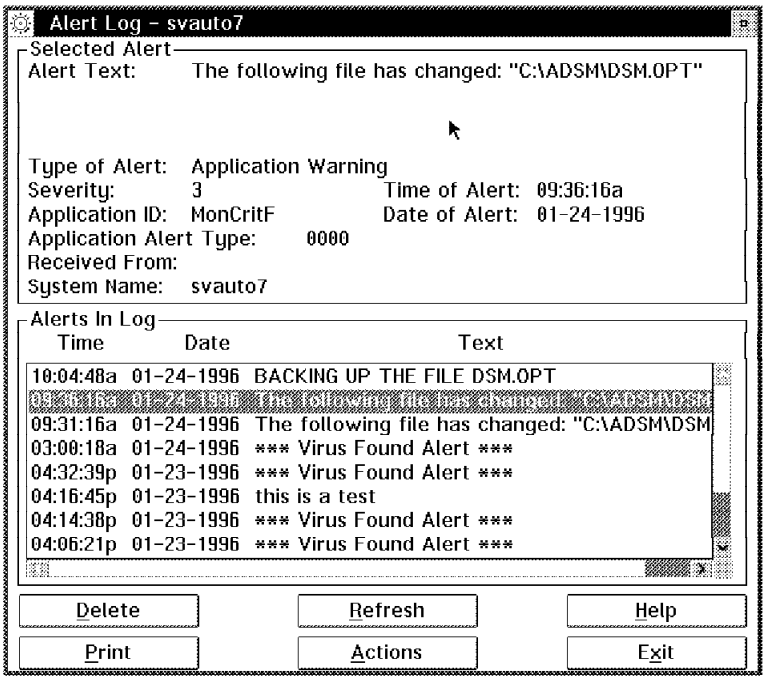


Figure 83. Alert Log

3.2.5 SAMPLE 2 Generating an Alert while Backing Up a File

In this sample we will use the genalert command to drive the process instead of one of the SystemView for OS/2 services like the Critical File Monitor. We will still be using the functions of SystemView for OS/2 and the Alert Editor. The following is a sample alert that we will use.

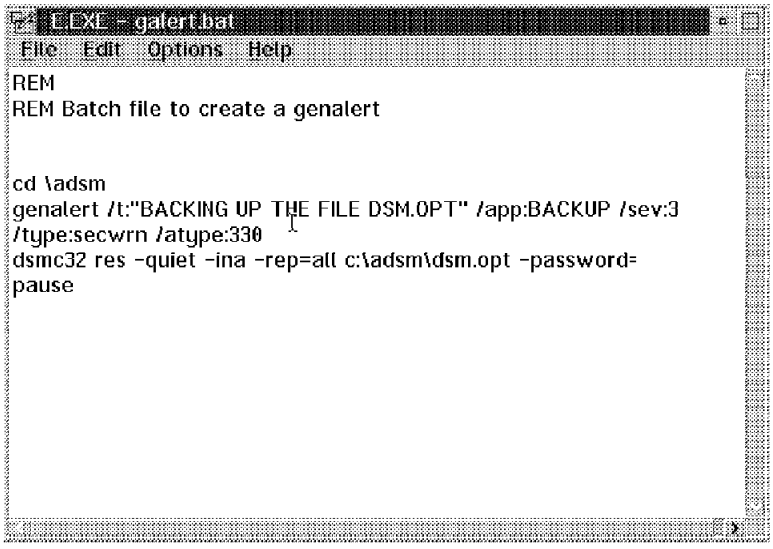


Figure 84. GALERT.BAT File

The BAT file is very simple and it will show up in the SystemView for OS/2 Alert Log. Notice in Figure 84 the Application ID and the Application Alert Type. They should match exactly what is in the genalert command.

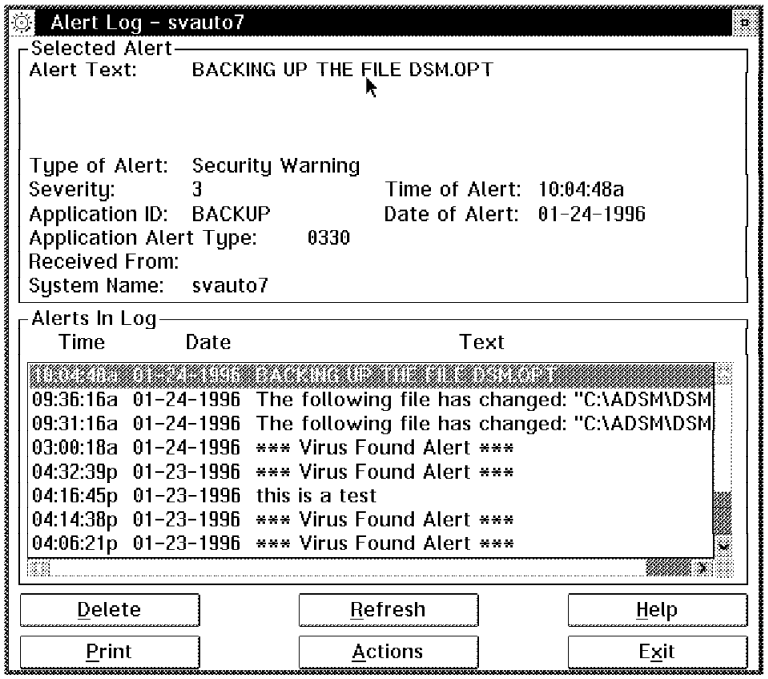


Figure 85. Alert Log

Once the genalert flows to the Windows 95 Alert Editor Service it will initiate the command SEL D:\ADSM\DSM.OPT, which will let you backup the file. This is now the same process as it was with the ADSM client for OS/2. The output from this command can be seen in Figure 86.

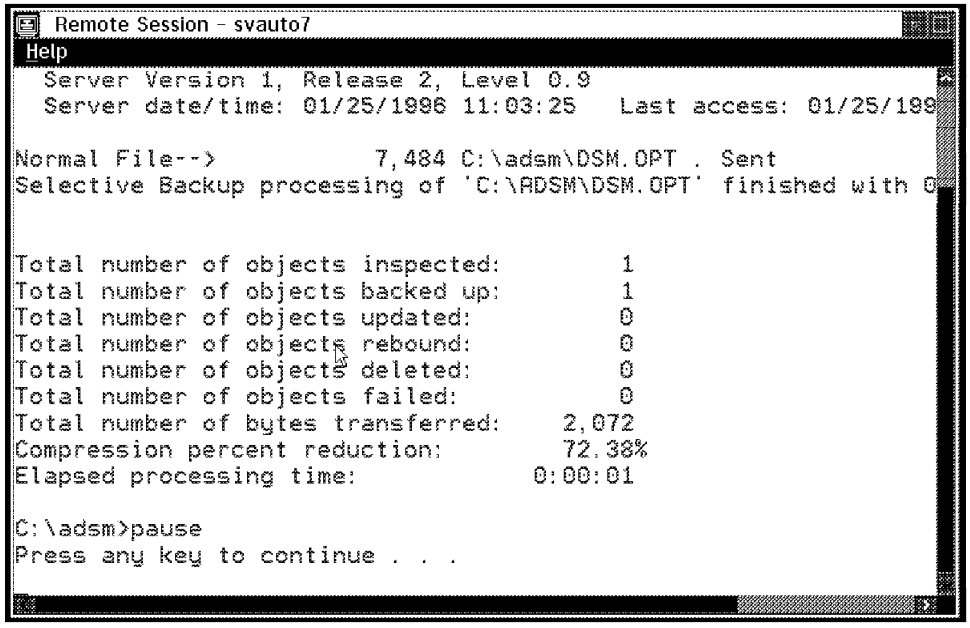


Figure 86. GALERT.BAT Execution

3.3 ADSM Client for NetWare

This sample deals with the following:

- Generic Alerts
- ADSM server and client configuration

The main intent here is to show how ADSM can be automated to perform some actions like backing up files through SystemView for OS/2.

3.3.1 Generic Alerts

In this sample we will be executing commands on the NetWare server. We can do this manually by entering commands at the console, or we can run batch files, using *NCF* files. The two processes that we are concerned with here are to keep track of the what actions have been performed from an ADSM perspective as well as a way to notify a systems administrator when these actions are taken.

The genalert is executed in a Novell environment and its structure is very similar to the one we use with Windows 95 and OS/2. The syntax for using genalerts follows:

```
* LOAD GENALERT /T:text /APP:id_name /SEV:0..7
               /TYPE:sssttt   /ATYPE:hexnum.
```

where:

- /T: - This field contains user text about the alert.
- /APP - Defines the application ID for the alert.
- /SEV - Defines the severity assigned for the system administrator for this alert.
- /TYPE=sssttt - This is the only field that should be filled in according to standards:

  SSS
  - UNK - Unknown
  - SYS - System
  - DSK - Disk or DASD
  - NET - Network
  - OS_ - Operating System
  - APP - Application
  - DEV - Device
  - SEC - Security

  TTT
  - UNK - Unknown
  - FLT - Fault or Failure
  - ERR - Error
  - WRN - Warning
  - INF - Information

  These values can be used in any combination.
- /ATYPE - Defines the application specific alert type as a hexadecimal value between 0000 and FFFF.

Note: When this was written, there was a bug in the NetFinity V3.05 code that runs on the NetWare server. It was not able to register in the alert log the alerts that came from the critical file monitor. This bug should be fixed quickly. Sample 3 shows the way it can be managed.

3.3.2 ADSM Client for NetWare

The installation process for the ADSM for NetWare client is more difficult then the OS/2 or Windows versions that we already worked with. Figure 87 shows the installation panel for ADSM after loading the NLM from the diskette.

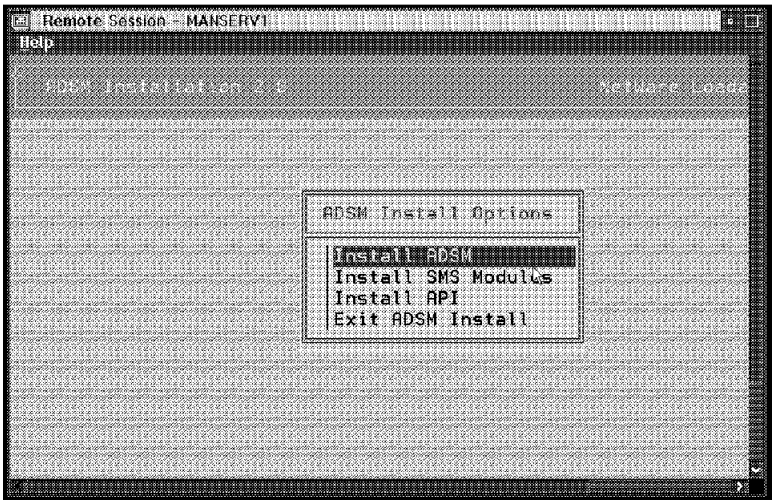


Figure 87. ADSM Client for NetWare

The installation process follows:

- On the NetWare console type LOAD a:\INSTDSM.
- Select the option **INSTALL ADSM**.
- Select the volume to install the code. We used SYS:/ADSM.
- A message informing you about the status of the installation will appear
- If the SMS Modules (second item to click on in Figure 87) are already installed you will not need to reinstall them. The install process will let you know.
- Once the files have been copied and the sms files loaded, you need to exit the ADSM installation option.
- In order for ADSM to be started automatically when the NetWare server starts, there are some statements that will need to be added to *AUTOEXEC.NCF*:
  * SEARCH ADD SYS:/ADSM
  * LOAD DSMC SCHED

  The last statement will allow ADSM to receive incoming requests to start scheduling processes.
- If you want to execute the new AUTOEXEC.NCF, you will need to unload and then load it from the console. Otherwise, it will take effect the next time you restart the NetWare server

  If you are running NetWare V4.1, you will need to load the following modules:

  – TSA410.NLM
  – TSANDS.NLM
  – SMDR.NLM

The above steps are required to get ADSM up and running. The next step is to modify the options file in the ADSM server and client.

The key configuration parameter we need to change for NetWare is the protocol. We needed to change the DSMSRV.OPT to use IPXSPX. The option file is shown in Figure 88:

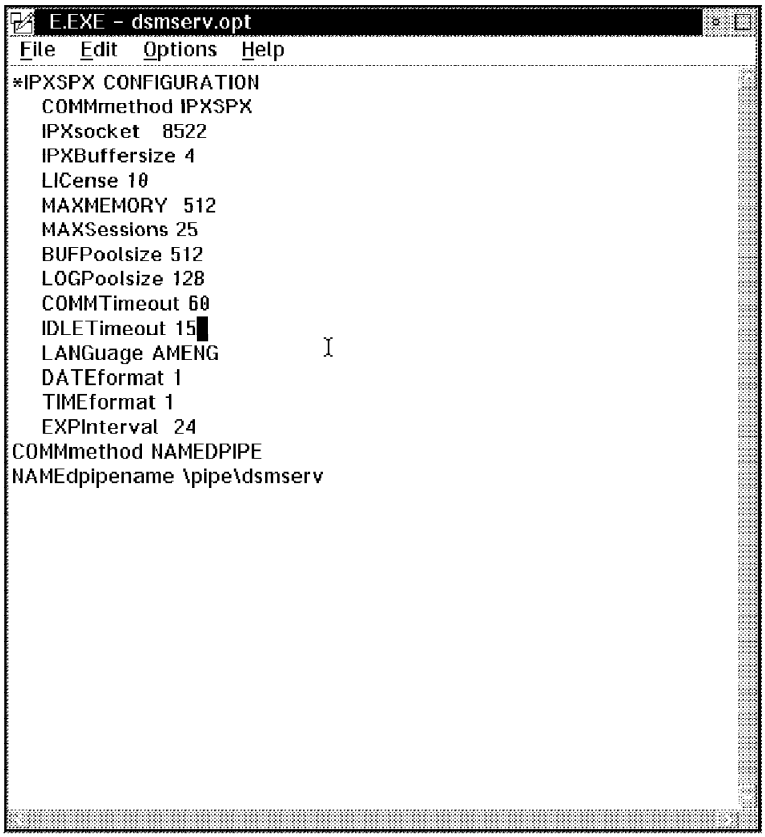


Figure 88. DSMSERV.OPT File

For NetWare, the key statements are:

- COMMmethod needs to be IPXSPX.
- IPXsocket must be the same socket that the client uses.
- License 10 means the number of license allowed for this server.

The options file, DSM.OPT, in the client should look similar to Figure 89 on page 69. In the client option file, the parameter IPXSERVERADDRESS indicates the netword ID and the address of the ADSM server adapter. Its format is NNNNNNNNAAAAAAAA. In this case:

- Network ID = 00000009
- Address ID = 400052005261

Another important parameter in the client DSM.OPT file is *NODENAME*. The value of this parameter needs to be the same as what will be in the command to register this node with the ADSM server. In this case, we called the node NOVELL.

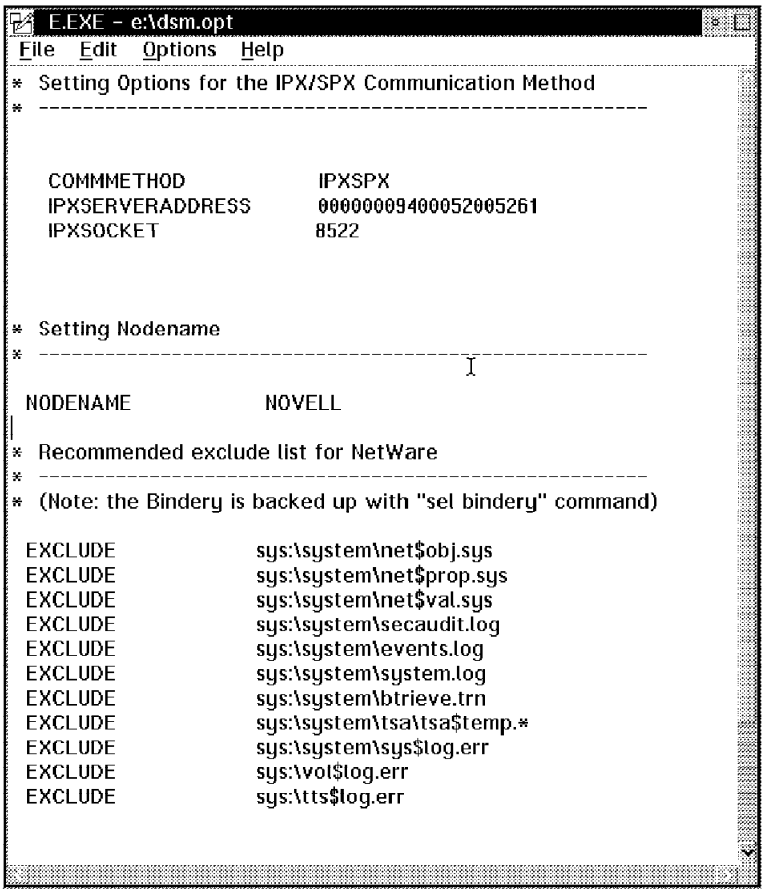


Figure 89. DSM.OPT File

Once you have modified the options files, you will have to register the node. This task is performed in the ADSM server with the following command:

* REG NODE NOVELL XXXXX SVAUTO

Here NOVELL is the name of the node, XXXXX is the password for this client and SVAUTO is the Policy domain.

3.3.3 SAMPLE 1 Generating an Alert while Backing Up File

The NetWare example is similar to the other examples. The only real difference is that the file type must be NCF in order to execute it on the NetWare server, and the syntax within the NCF file requires the LOAD parameter to precede the commands. Figure 90 on page 70 shows the program we created in order to receive the alert when a RESTORE command was issued.

Figure 90. GALERT.CMD File

The format of each of these commands has been explained in the previous sections of this chapter. When you execute this NCF, the program will generate an alert similar to the one in Figure 91.

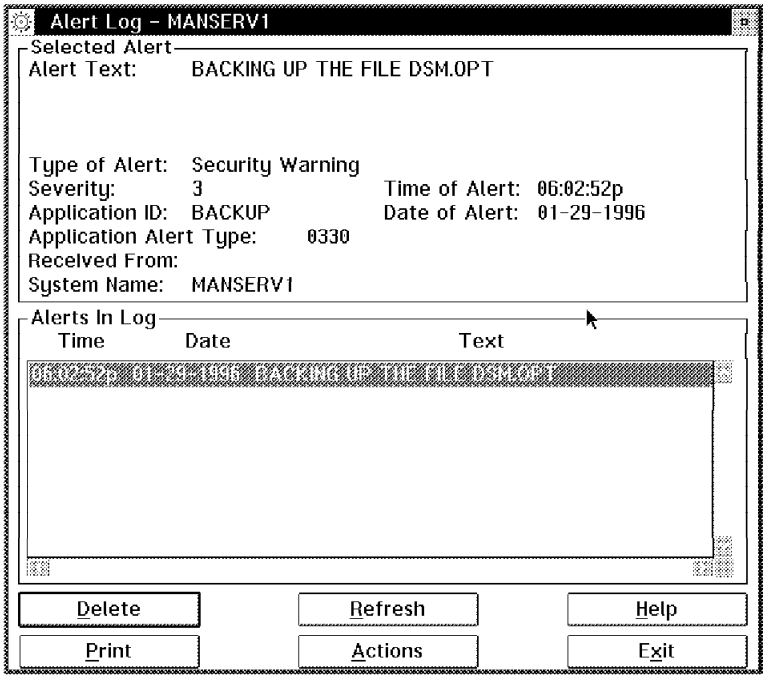


Figure 91. Alert Log for Command GALERT

As a result of the alert, the following two screens, Figure 92 on page 71 and Figure 93 on page 71, show the results. Note that the title bar on each of the figures shows it running in a remote session window.

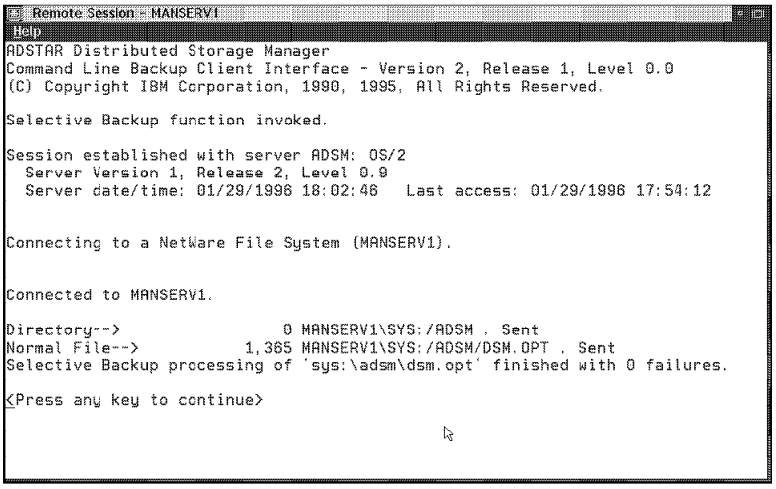


Figure 92. GALERT.NCF Execution

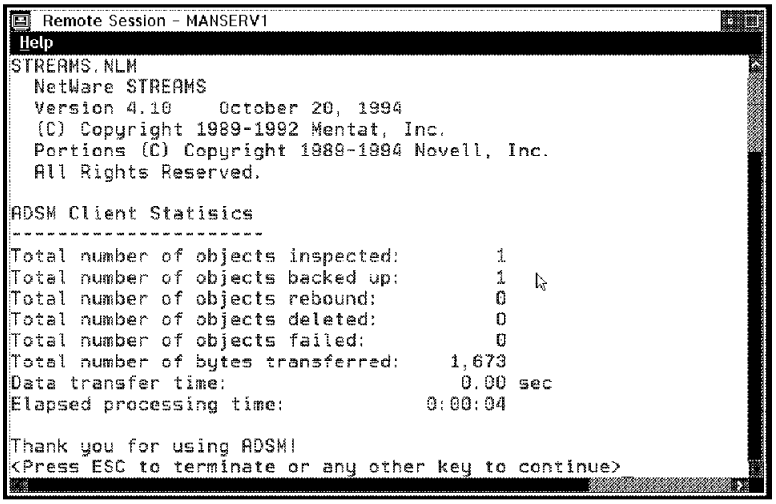


Figure 93. GALERT.NCF Execution Second Part

Alerts will not show up on the NetWare server. They will show up at the SystemView Manager. Therefore, you have to remember to add the IPXSPX or TCPIP protocol to the SystemView for OS/2 configuration in order to see the alert show up in the Alarm Log.

3.3.4 SAMPLE 2 Integrating ADSM into the Alert Manager

This sample shows how a genalert command can be associated with an action defined in the Action Editor service.

There are two components to work with in this scenario:

- Action Editor
- Genalert Command

The genalert command in this sample can be seen in Figure 94 on page 72. It is important to note the parameters used with the genalert command because those same parameters will be used in the filtering process in the Action Editor.

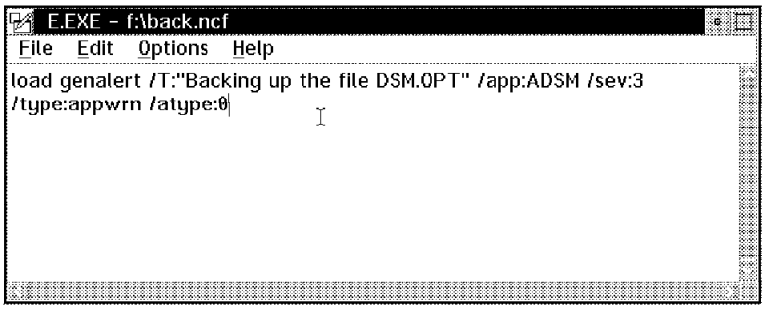


Figure 94. BACK.NCF Program

Since we know the fields in the genalert, we can set up our filter as shown in the following figure:

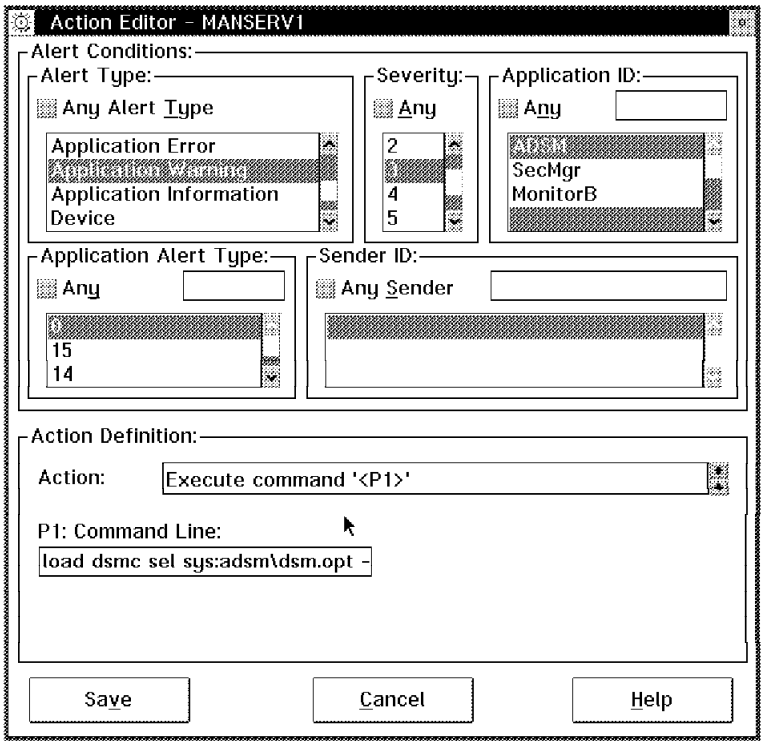


Figure 95. Action Editor

Depending upon the level of automation you wish to implement, you can either put the ADSM command right into the command line in the Action editor, or you can put it in an NCF file to be executed. In this case the action is the command LOAD SEL SYS:ADSM\DSM.OPT Password=xxxxxx.

If you execute the NCF command BACK on the Netware console, you will get Figure 96 on page 73 showing the alert log.

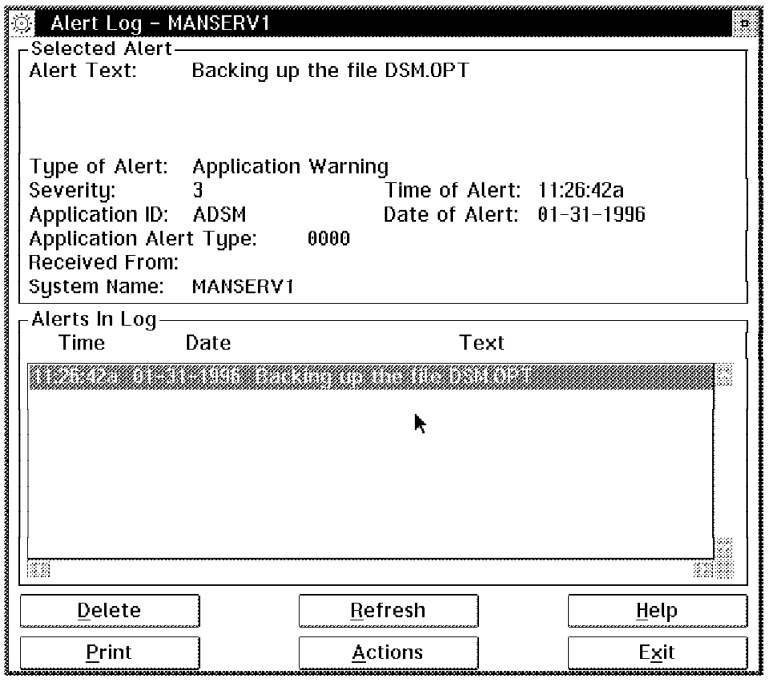


Figure 96. Alert Log NetWare Server

Once the alert flows and the program runs, the results will look something like Figure 97.

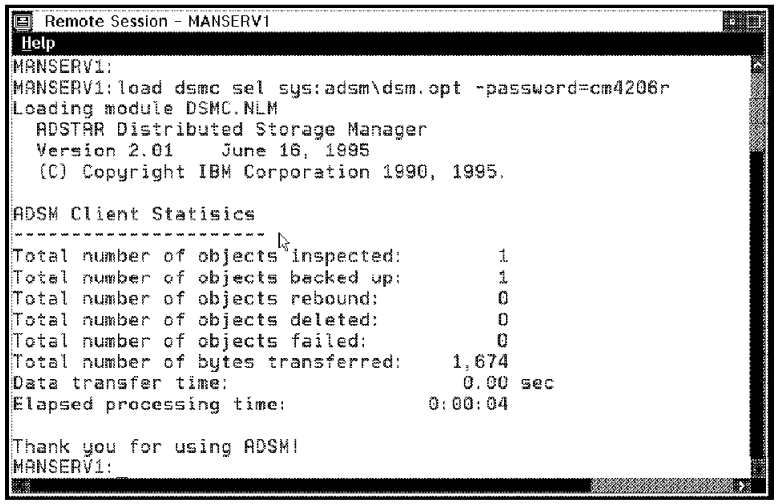


Figure 97. BACK.NCF Execution

3.3.5 SAMPLE 3 CFM NetWare Alerts into Alert Log

The intent of this example is to show you how you can trigger some actions in the NetWare server once the file you are monitoring (using the Critical File Monitor) detects a change.

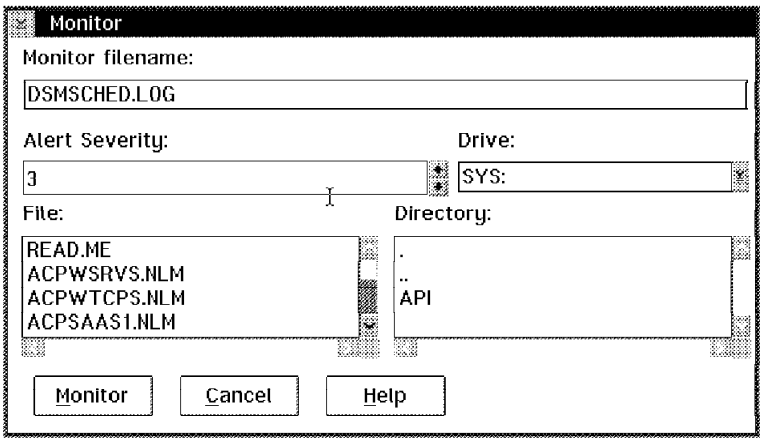


Figure 98. Critical File Monitor NetWare Server

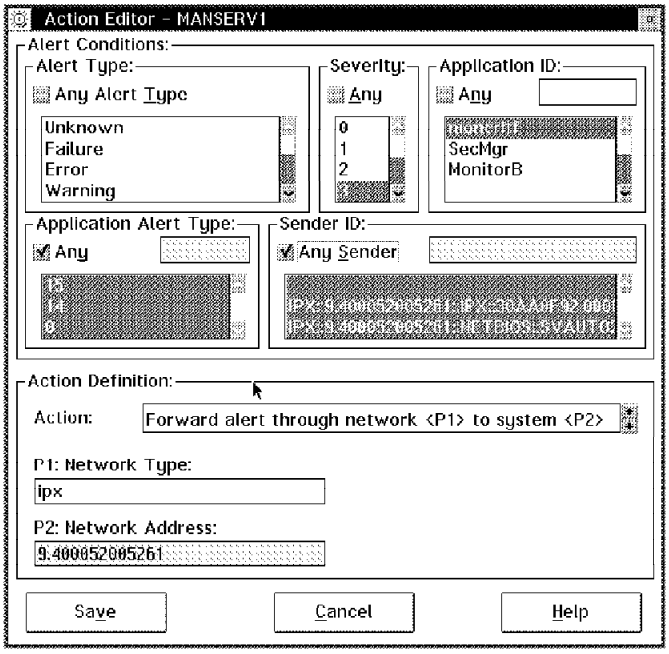


Figure 99. Action Editor NetWare Server

Once the alert gets to the SystemView for OS/2 server, it needs to interact with the NetWare file server. This is done using the Action Editor. You will need to go through the Remote Systems Manager and manage the NetWare server NetFinity client. Then you use the Action Editor service for the client on the managers GUI.

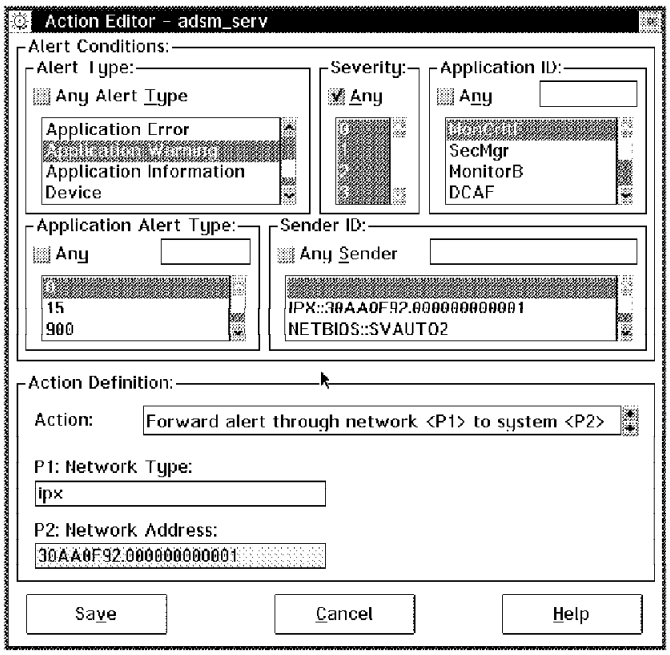


Figure 100. Action Editor SystemView Server

Since we specified in the Action Definition to **Forward alert through network <P1> to system <P2>** it will show up on both systems. Notice in Figure 101 that the field *Received From* indicates the IPX address of the system the alert came from.

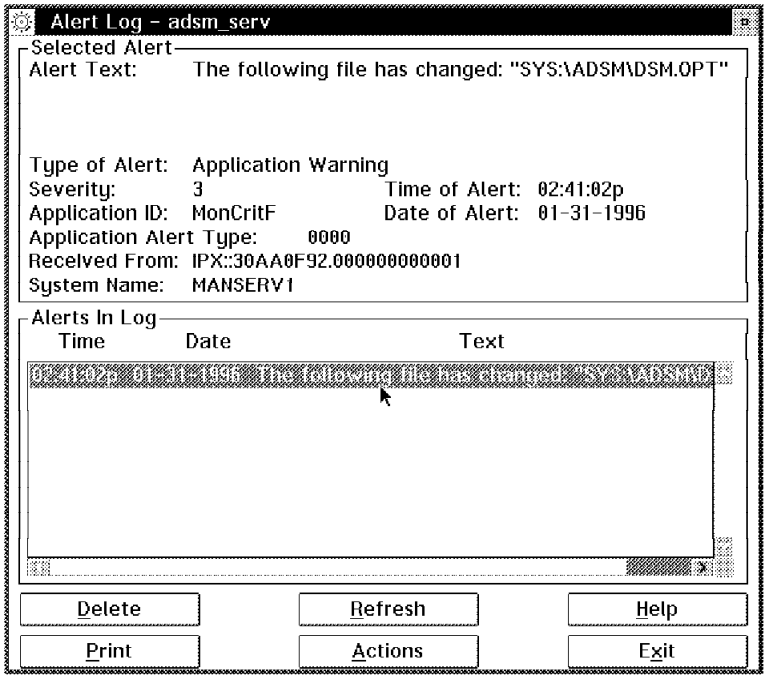


Figure 101. Alerts from SystemView Server

In the alert in Figure 102 on page 76, you can see how the alert is doing a loop. The alarm comes from system 9.400052005261, which is the SystemView Server, but this alert is being attached to the NetWare server.

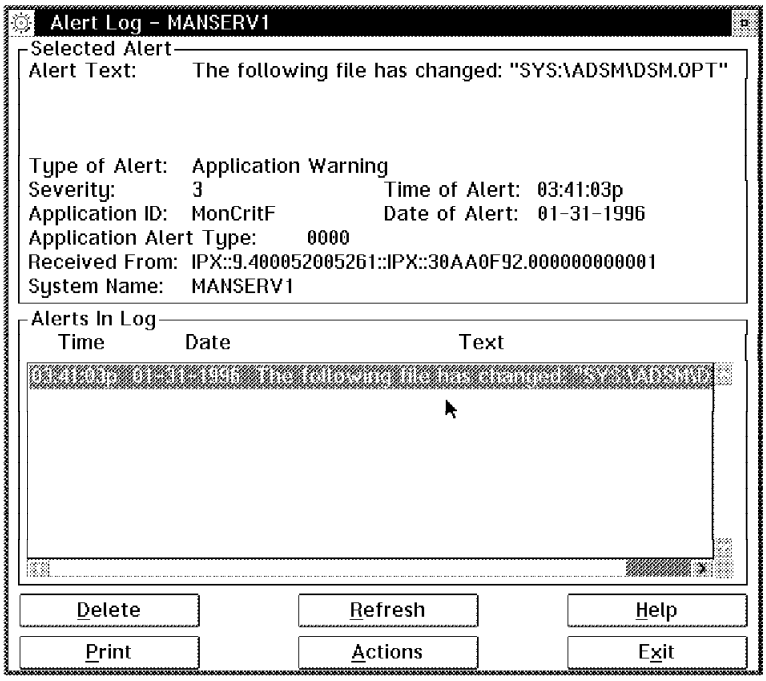


Figure 102. Alerts from NetWare Server

Chapter 4. Automating Software Package Install

This chapter showssome integration between a user change request coming in using Genalert and automatically updating a software package.

This chapter deals with the following steps:

1. SystemView Preparation
2. Software Preparation
3. Software Inventory
4. Evaluating product version
5. Generating Alerts and Starting Distribution Process

4.1 SystemView Preparation

For this chapter we used two machines SVAUTONV and SVAUTO2. The procedure used for the installation of the manager, SVAUTONV, was to install:

- SystemView Administrator Console code
- Software Distribution Server
- Software Distribution Object Preparation

For the client, SVAUTO2:

- SystemView Client Graphical Interface
- SystemView Client
- Software Distribution Object Preparation

The options to be installed are dependant upon whether or not the client will be an active or passive client. If this machine is configured like an active client it will be able to pull software code from the server; if it is passive, it will only receive requests from the server.

The installation process is shown in Figure 103 on page 78.

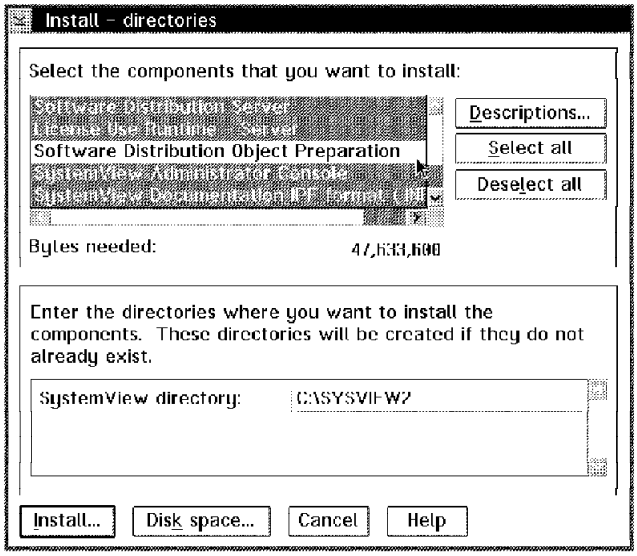


Figure 103. NVDM Server Installation

The setup of the server is very simple. You only have to select a valid transport protocol from the SystemView configuration notebook. This notebook is found in the SystemView folder. The second page in the notebook shows the other directories that are related to the software distribution setup.

An example of the configuration for NVDM.CFG is shown in Figure 104. This file is stored in the SYSVIEW2 subdirectory and contains the main parameters related to NetView Distribution. Some of them are susceptible to change, like the number of user interfaces and maximum number of targets, We didn't change the name of the server or the protocol used. This kind of operations can be done in the configuration notebook in the SystemView for OS/2 folder.

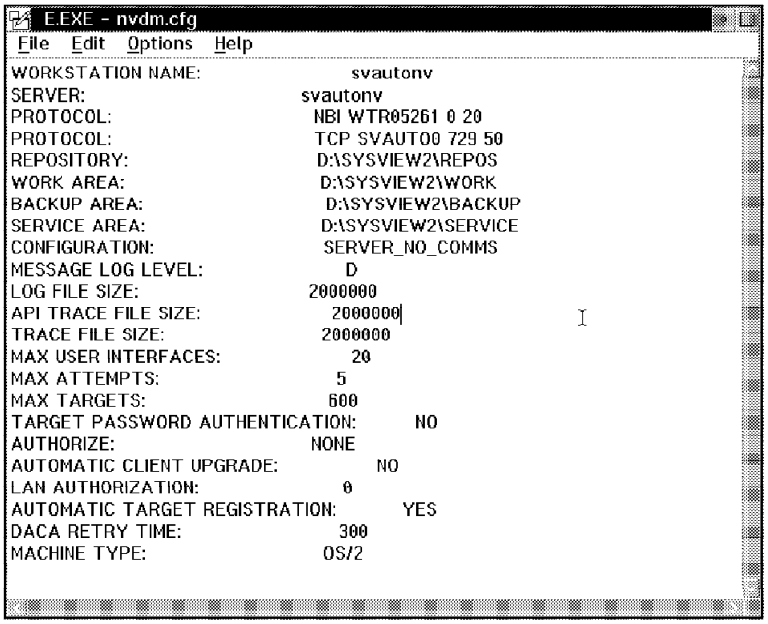


Figure 104. NVDM.CFG Server File

The configuration file for the client is similar to the server. Figure 105 on page 79 shows what the client looks like. The main difference is the structure of the client name. You can see that it is made up of the name of the system, the protocol used, and the address of the client. The sample in Figure 105 on page 79 shows the names without a period in between the fully qualified name. That is just how it is shown in the window. When you reference it, you will need the periods.

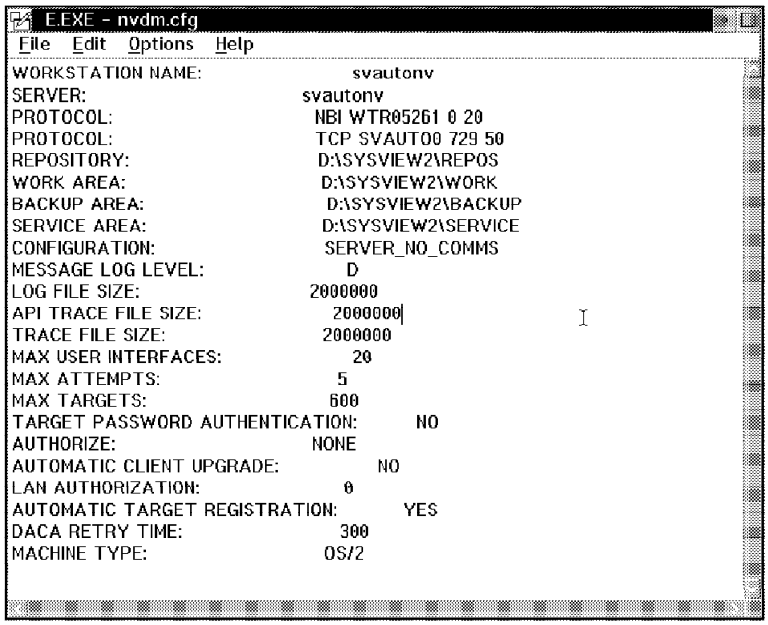


Figure 105. NVDM.CFG Client File

The protocol parameter will determine how the distribution takes place. Even if SystemView for OS/2 has multiple transport protocols, if you don't specify the protocols in the NVDM set up, you will not be able to use those transport protocols.

Important

Most of the information typed in the notebook *is* case sensitive.

After following the above steps, the server should be set up. The registration is performed automatically for you. If you want to see which clients have been registered with the server, you can use the following commands:

- NVDM LSTG
- NVDM STATTG

The first one will show you who has been registered with the server, while the second one will show if the client is available or not.

If the NVDM client does not appear in the list, you will have to issue the following command:

- NVDM SVR

The above command will register the NVDM client with the server defined in the file FNDADMN.CLI in the path d:\SYSVIEW2\UICFG.

4.2 Software Preparation

There are three procedures involved with the setting up of the Software Preparation function:

- Generic Applications
- CID Software Preparation
- Application Sharing

The main goal of this section is to go through the first two methods in order to create software packages ready to be distributed. In our samples we are using two software applications, PMCAMERA and ADSM for OS/2. In order to get the first one installed you only have to copy the executable files, there is no modification to the CONFIG.SYS or to the AUTOEXEC.BAT, so in order to be distributed a Generic Package needs to be constructed; the ADSM for OS/2 is a little different it needs some additional information, like path, update the config.sys, etc. so if you want to distribute a software package like this you will need to through the CID installation in order to install the package in an unattended way.

4.2.1 Generic Applications

The process is quite simple. There are four main components as follows:

1. Define Files
2. Define Variables
3. Register Scripts
4. Establish Characteristics

When you create a software package you need to create a name for the package and a place to put the software. In addition, there will be a description of what the package is. In order to do all of this, you will need to use the following components of SystemView for OS/2s GUI:

- SystemView Service Manager
- Software Preparation
- Software Preparation Option Software (new)

For Software Preparation Option Software, there are three options:

- Files
- Variables
- Scripts

Each one of these will allow us to define where the application is that we want to distribute, what kind of variables we are using, and the files needed in order to let the NVDM target know about what has to be done before and after putting the files over the target directory.

These scripts allow you to execute a CMD program in the remote target before or after the software package has been sent. In this sample we are working with a package that is not able to create an icon on the desktop so we have to install a CMD program in order to get the folder and the object in the desktop.

In Figure 106 on page 81, it shows the window where the name of the object should be entered. If a global name is not provided, the default name will be this one.

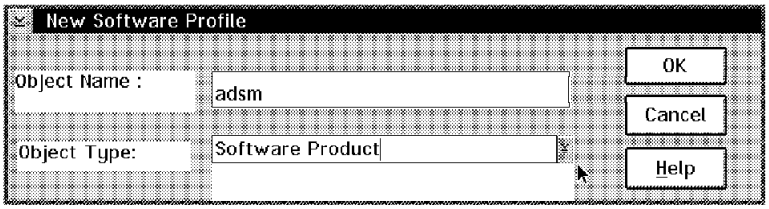


Figure 106. New Software Profile

As soon as you enter a name, a new window will appear showing the icons we have already talked about for files, scripts and variables.

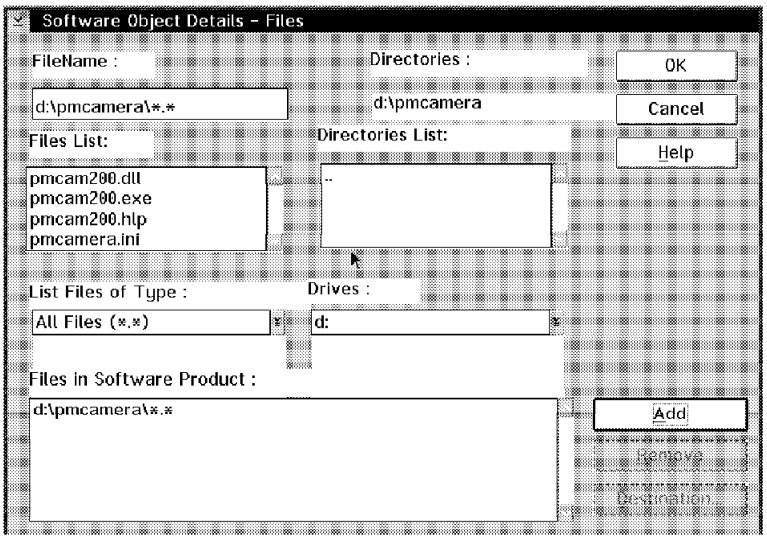


Figure 107. Software Object Details

By clicking twice on each icon, we get the parameter window.

For the File option in Figure 107, the process is as follows:

- Select the driver where the software is located.
- Select the directory or file to be distributed.
- Click on **Add**.
- Click on **Destination**.

The last step looks similar to Figure 108 on page 82.

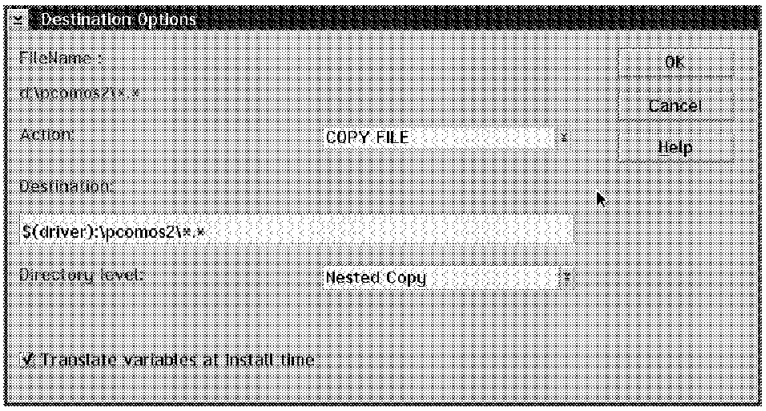


Figure 108. Destination Options

Here you define where this information will be stored on the target and what level of distribution will be done.

For this sample, the destination will be as follows:

- $(driver):\pcomos2*.*

Here $(driver) is the name of a variable that will allow us some flexibility at installation time. The rest of the sentence is the target path. In order to copy not only the main directory but all of the nested directories, you should specify that and also the option for translating variables as follows:

- Directory Level = Nested copy
- Translate variables at install time should be marked

Some times it is convenient to use variables instead of using a specific location. With a symbol, it is easier to change things like the target drive, the install directory or other options. The setup for the variables is as follows:

From the preparation object details GUI:

- Click on **variables**.
- Write down the variable name. In this case the unique variable is drives. The text here is case sensitive.
- Assign a value.
- Click on **Set**.

Figure 109 on page 83 shows an example of this.

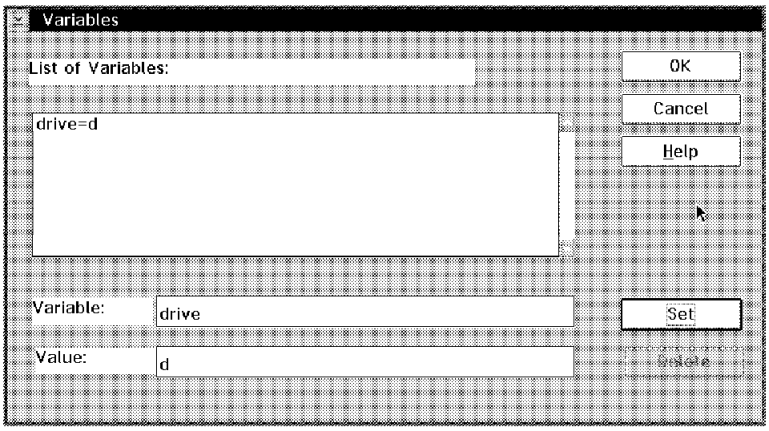


Figure 109. Variables Settings

The generic applications doesn't have the capability to create icons on the desktop, so for this sample we are going to need to execute a CMD file in order to create the icon for the PM Camera application. This command must be run after copying the software application files.

Figure 110 shows how to setup the Scripts section.

- Choose how the script will be installed. The choices are:
  - Before installing the application files
  - After Installing the application files
- Type the name and path of the exe. For example:
  - `$(drive)&colon\icon.cmd`

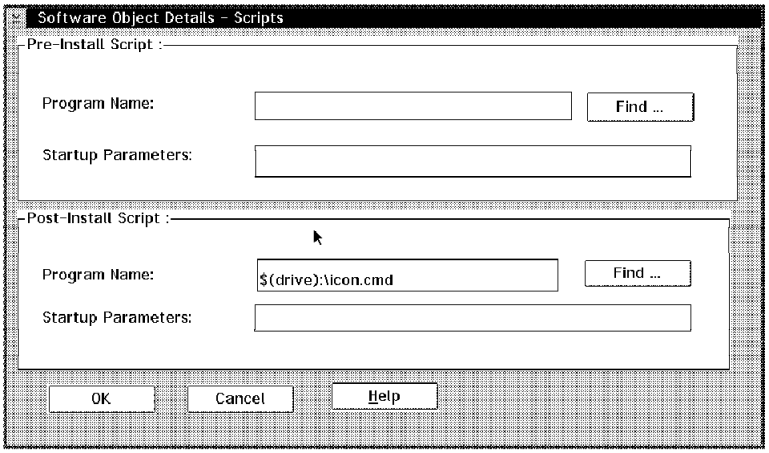


Figure 110. Script Definition

You also can search for the name of the command if you use the find option.

In this sample, the REXX program is in ICON.CMD. It will create a folder containing an ICON with the PM Camera Executable.

Some details on this program are shown in Figure 111 on page 84.

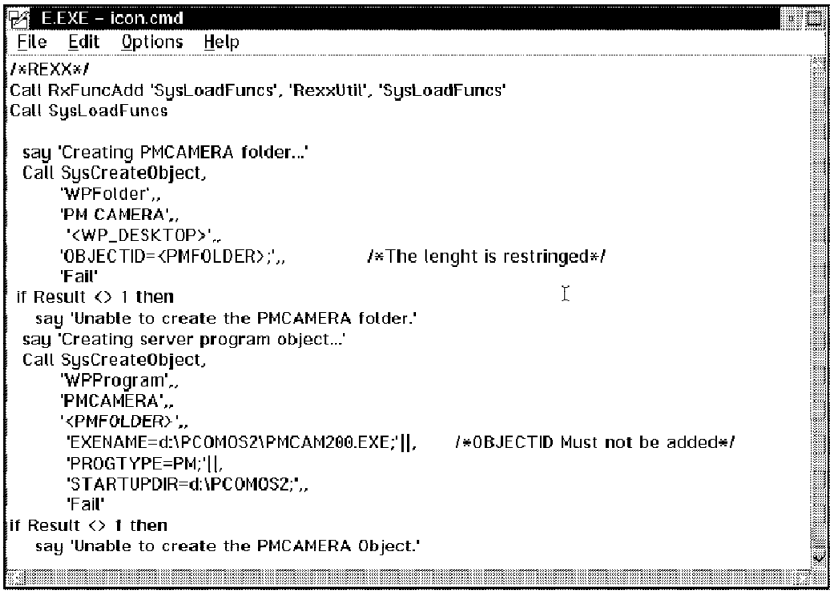


Figure 111. ICON.CMD

The last step is to generate a Global Name. A global name is used to help you recognize your software package in the repository database. The Global name is composed of four tokens:

- NAME.TYPE.LEVEL.VERSION
  - Name - Indicates the name of the software to be installed.
  - Type - This can be refresh, update or fix.
  - Level - This represents the level of the code.
  - Version - This represents the version of the code.

The steps to set it up are as follows:

From the Preparation Object Detail window:

- Click on **Options**.
- Click on **Characteristics**.
- Enter your values.
- Click on **OK**.

The above steps are summarized in Figure 112 on page 85.

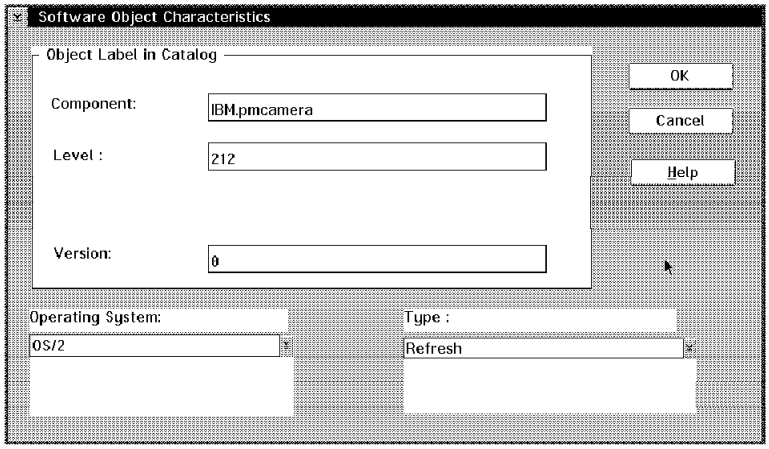


Figure 112. Global Name Definition

Once you have defined it, the software package is ready and the window can be closed.

The last step is to catalog this package. The steps are as follows:

From the Software Preparation Profiles window:

- Click once on the object that represents the software package you just created.
- From the menu bar click on **Software**.
- Click on **Catalogue** and wait for a message.

The message should look like Figure 113.

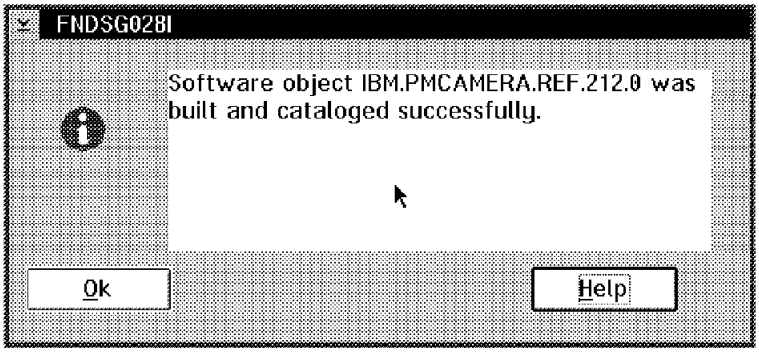


Figure 113. Pop-Up Window for Cataloged Products

4.2.2 CID Applications

This part deals with the software package preparation using CID techniques. We use the following elements:

1. Network Operating System
2. ADSM CID files
3. SystemView for OS/2 CID Preparation

In the distribution of software packages there are at least three elements. In our case we had the NVDM server distribution, NVDM agent and the Code Server. The last one is really very important because it implies a machine that is able to keep the images of the software we are distributing. This machine is called a code server because in order to get that code to other machines, a Network Operating System will be needed. This means that the code server will be able to maintain the software images and share them with the requester. In this case, it will share it with the NVDM client.

The NOS available for SystemView at this writing were:

- LAN Server
- NetWare Server
- SRVIFS
- NFS

The sample showed in this chapter was implemented using NFS.

The software package to distribute was ADSM, a complete list of CID enabled products has been attached in one of the appendix.

SystemView has built using a utility called CID Software Preparation in order to create the necessary elements for the distributing process.

We will show all of the processes that go into this.

4.2.2.1 NFS Setup

For OS/2 TCP/IP version 2.0 you will have to install the NFS kit since it is not included in the base kit. For OS/2 TCP/IP version 3.0, NFS is part of the base.

The setup for NFS is quite simple and it is detailed below:

1. Select the machine that will provide the storage for the software images. You will have to create the file structure.
2. Enable NFS Daemon in the Code Server.
3. Enable NFS Support in the NVDM target.
4. In the code server, establish the name of two directories for the images and the logs.
5. In the code server, add the names of the hosts allowed to mount those directories.
6. Save the configurations in the NVDM targets and in the Code Server.

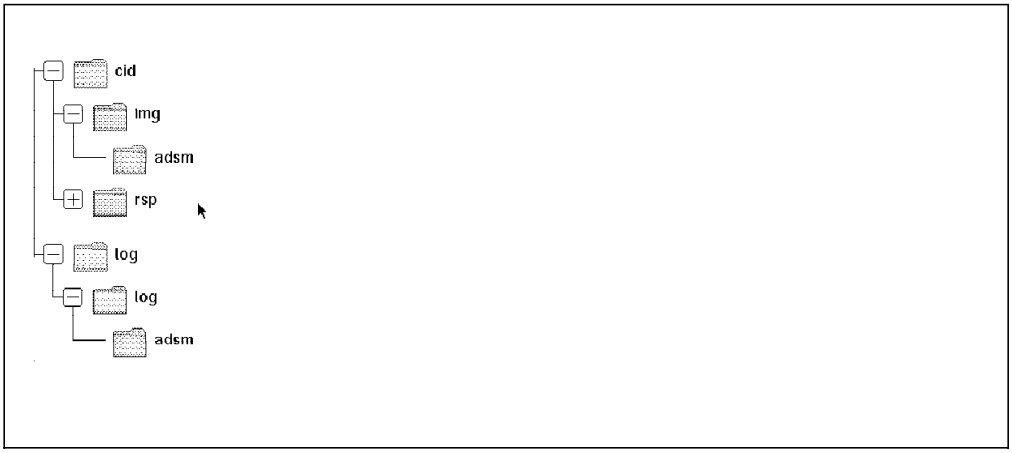


Figure 114. Directory Structure

- This machine should be a machine with enough space to store information for the logs and software package images. A directory structure needs to be created and it should look something like Figure 114. The CID preparation doesn't take care of creating the directory structure. It will only use the information stored there.
- In the configuration of TCP/IP, there is an option to autostart some services. You will have to select the **NFS** service.
- For the NVDM target, it is not necessary to enable the NFS daemon. The NFS control program will be enough.
- NVDM requires two places to store the software and the logs. The structure for these directories is as follows:
  - D:-CID-IMG-ADSM for Software Images
  - D:-LOG-LOG-ADSM for ADSM logs

Only the parts D:-CID and D:-LOG have to be registered in the NFS notebook on its page two (as shown in Figure 115).

The sub-directories IMG and LOG are not required but are names that people often use.

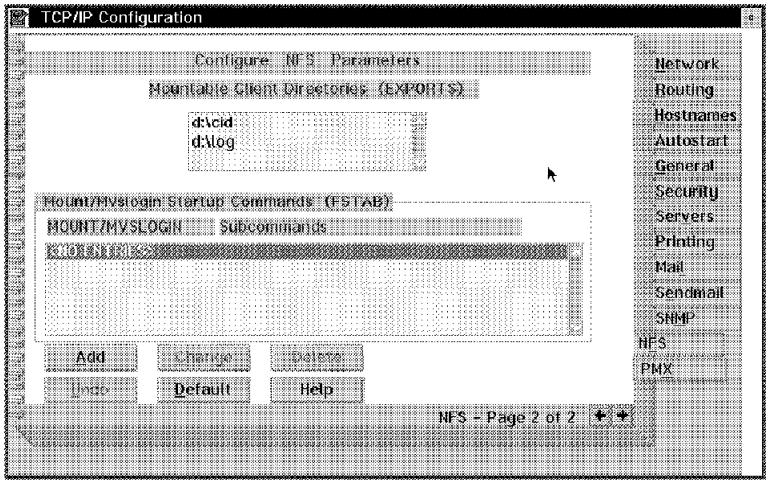


Figure 115. NFS Notebook

After selecting the directories, you can use the panels to determine who has access to them and what restrictions there are on the files within them. This relates to the kinds of permissions that are available for the files: read or write access. Both of the directories (images and logs) will be added to the NFS EXPORTS file. The location of the EXPORTS file is determined by a symbolic variable called ETC that is located in CONFIG.SYS.

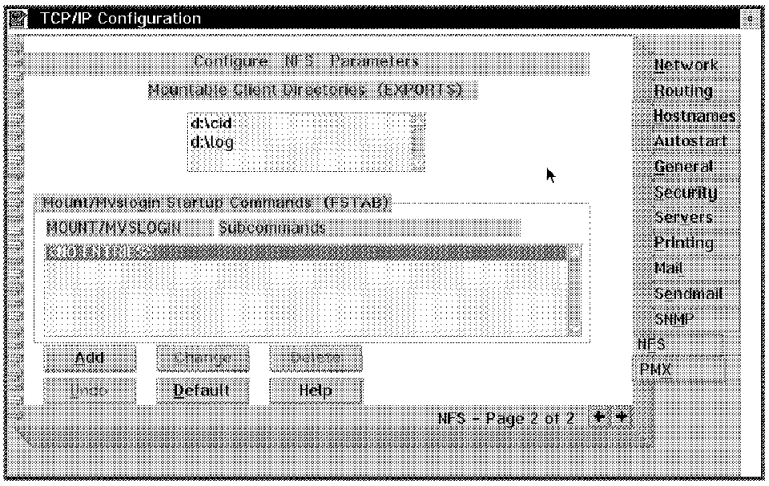


Figure 116. NFS Hosts Access

When you set up your configuration files in the SystemView for OS/2 notebook, you will reference these same directories.

4.2.2.2 CID Setup

The setup for the CID process is a little more complex, it mainly deals with the following:

- Configure CID Notebook
- Copy product images to the Code Server
- Build file XXXX.ADF
- Build file XXXX.MRF
- Build file XXXX.VAR
- Add Software Package to the library
- Catalog the software package

The relationship between these files is shown in Figure 117 on page 89.

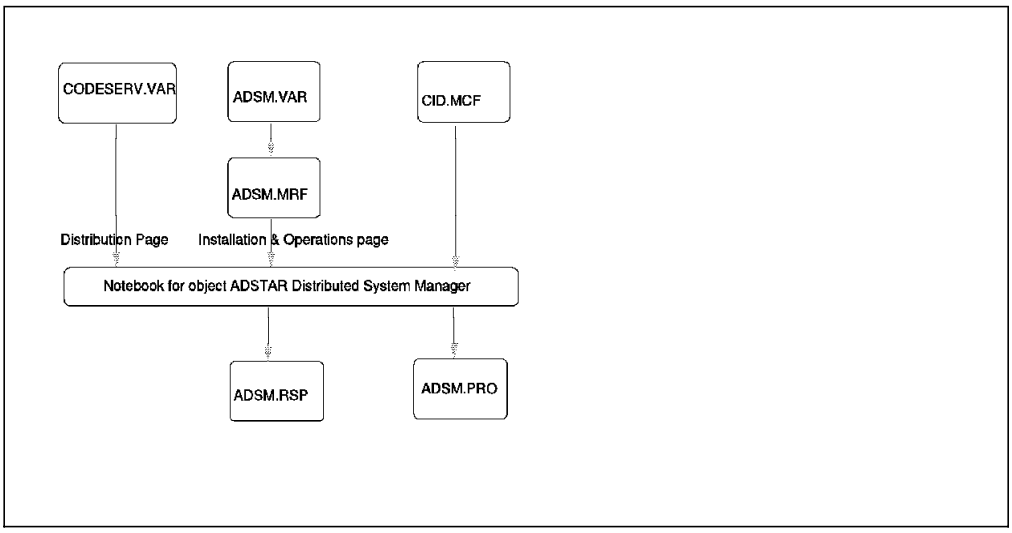


Figure 117. CID File Interaction

Once you have started SystemView double-click on the **CID Software Preparation** icon. From there, your first step is to go through the Code Server Setup utility. Figure 118 shows the new notebook.

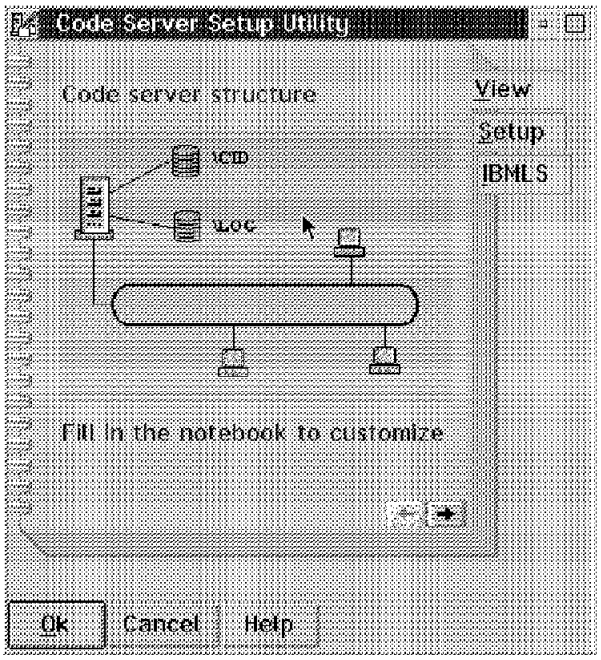


Figure 118. CID Software Preparation

There are four main parameters with which the code server utility works.

- Type of redirection
- Code server name
- CID directory
- LOG directory

These functions are shown in Figure 119 on page 90.

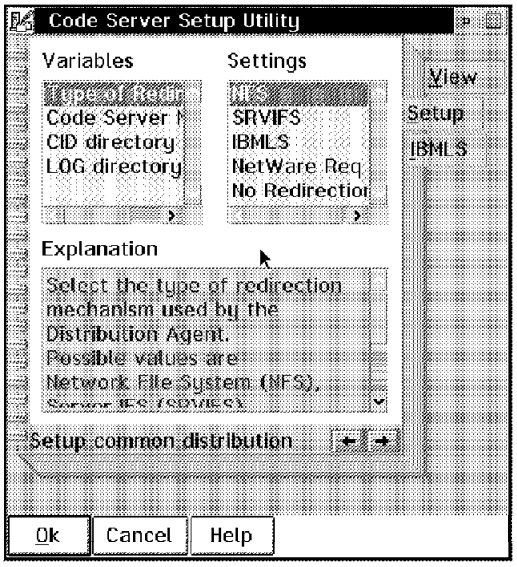


Figure 119. CID Notebook

- Type of redirection - Refers to how the SystemView client accesses the software images and logs in to the code server. There are several ways to communicate with the server. We implemented NFS in this scenario.
- Code Server Name - Since we are using NFS for our connection, the code server name will be the TCP/IP hostname. This name can be found in CONFIG.SYS, or in the TCP/IP configuration notebook.
- CID directory - This is the same directory that we placed in the NFS EXPORTS file in the previous section. The structure of the directory is shown in Figure 114 on page 87 and below:
  - D:\CID\IMG\ADSM*.*

  From a data entry perspective you will only need to enter ADSM for the directory. The other pieces of the file structure are built from NFS (D:\CID) and from the standard (IMG). The LOG directory works in a similar manner.

Once you have updated this notebook the next step is to copy the images for the product that is being distributed into the correct source location.

The next step is to build the files necessary to distribute the software package.

There are four types of files we need. They have file name extensions of ADF, MCF, MRF and VAR.

- ADF stands for Application Definition File.
- MCF stands for Model Change File.
- MRF stands for Model Response File.
- VAR stands for Variables.

The first one has 4 main sections:

- Mandatory Variables
- Configuration Variables
- Model Change File

- Model Response File

The interaction between them is very interesting and its purpose is to generate two kinds of files:

- Change files
- Response files

The first one will let you to distribute a software package. It has all of the instructions, variables and options that are needed to install the package.

The second set of files (response files) allows you to install the change files in unattended mode. A very positive feature of SystemView for OS/2 is that during the set up process, this file can be generated automatically. Also, instead of having one response file for each machine, we only will have one Model Response File and one Model Change File.

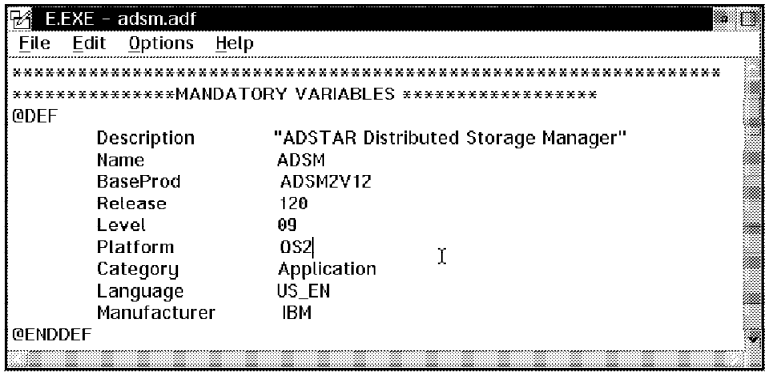


Figure 120. ADSM.ADF Mandatory Variables Section

The *mandatory variables* section in Figure 120 contains information about the global name of this product. The global name structure is as follows:

- Manufacturer.BaseProd.ID.REF.release and level.Language

Each one of these options, except the third and fourth token are taken from this section. All the tokens are case sensitive.

This long name is built for the CID.MCF. That is a standard file that you do not have to change. Figure 120 shows what this should look like.

The next section, the Configuration Variable Section, is related to the paths needed.

- It shows where the INSTALL.EXE program is located.
- The path for the Software Images.
- The path where the logs are going to be kept.

Figure 121 on page 92 shows how this is set up to work with ADSM. In the same figure (Figure 121 on page 92) there is a sentence called @INCLUDE CODESERV.VAR.

This file is standard for all ADF files and its purpose is to create a notebook with the values gathered from the ADSM.VAR and ADSM.MRF. This notebook will be completed during the cataloging process.

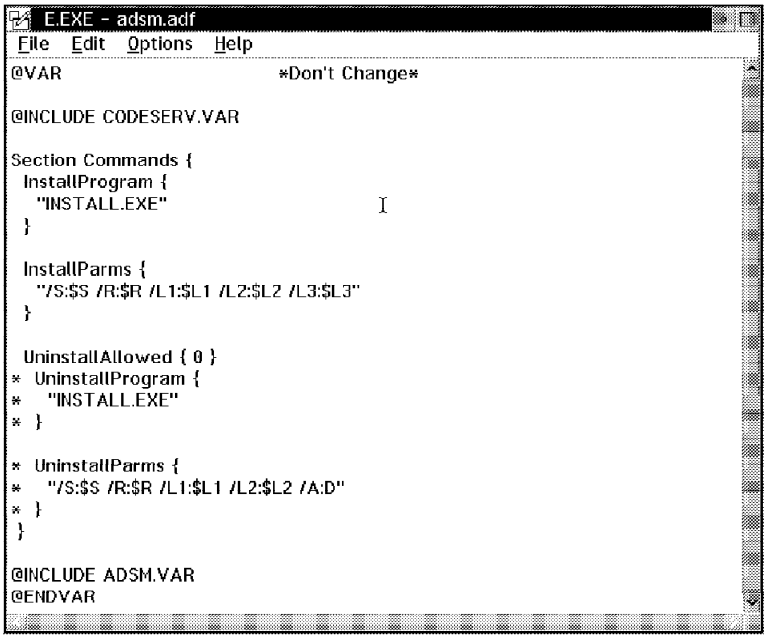


Figure 121. ADSM.ADF Configuration Variables Section

In Figure 121 there is also a section at the bottom for the ADSM.VAR file. That is used to translate the variables from the ADSM.MCF into real values.

The last two pieces point to the files ADSM.MCF and ADSM.MRF. These two files will generate the change file and the response file. Figure 122 shows this section.

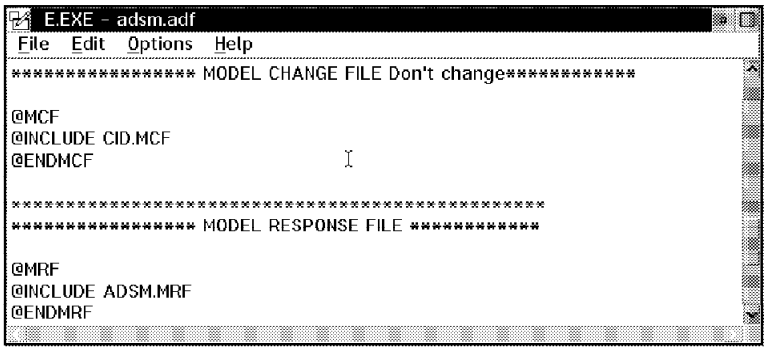


Figure 122. ADSM.ADF Model Change and Response Files

In order to build the file ADSM.MRF, we need to find a file model. Normally, if the application is CID enabled, the software should contain a file with an extension of RSP or DAT. This file can be used as a model and changed to allow managing variables values. Figure 123 on page 93 and Figure 124 on page 94 shows how the file should look.

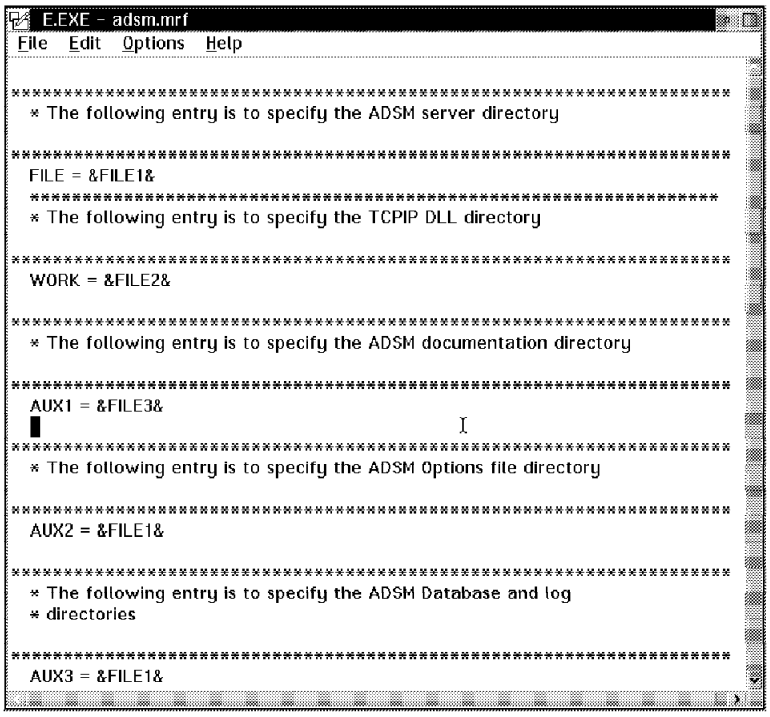


Figure 123. ADSM.MRF File

As you can see, most of the values are variables that will be resolved using the ADSM.VAR. All the variables begin and end with an ampersand.

Figure 124 on page 94 shows the next part of the same file. We can see the variable COMP and also some information that indicates which applications will be installed. The VAR file will help resolve the values.

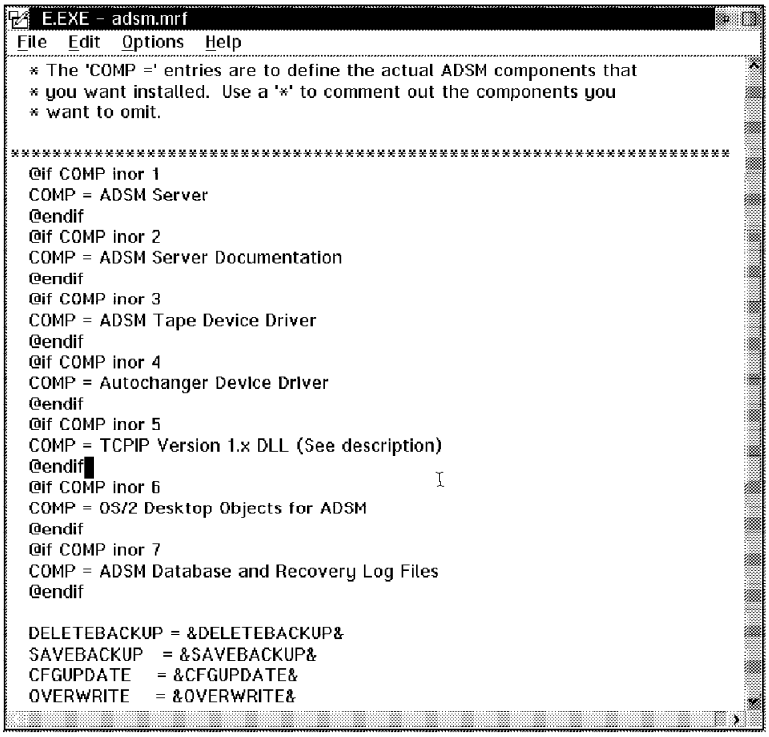


Figure 124. ADSM.MRF File 2nd Part

The paths that are needed to finally delete the backup copies and the updates will also be provided in the ADSM.VAR file.

Each variable in this last file have to be defined in the VAR file, As you can see, a default value is assigned to each variable. Figure 125 on page 95 shows the value for the variables FILE1, FILE2 and FILE3. Figure 126 on page 96 shows the variables for the installation process.

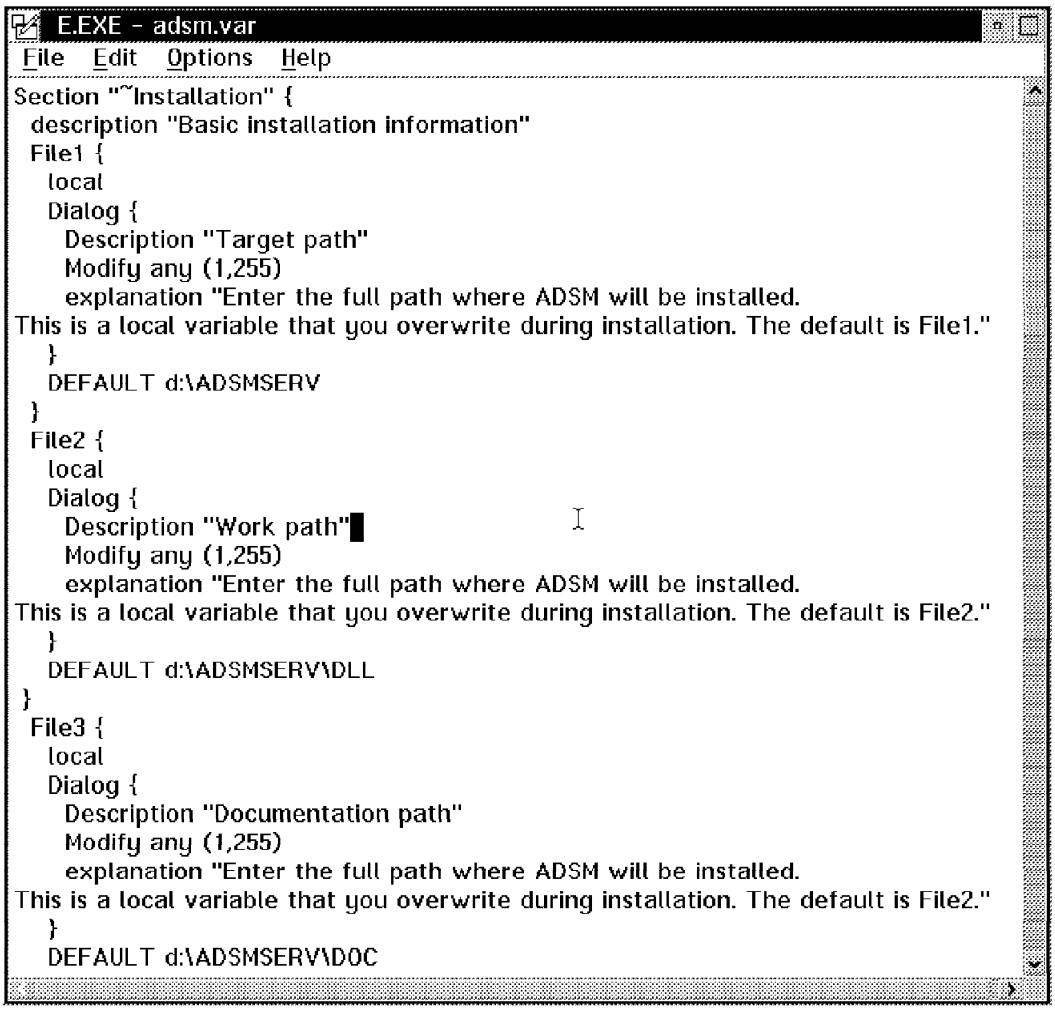


Figure 125. ADSM.VAR File Part 1 of 3

The second half of the figure has definitions for the components to install and the proper default values.

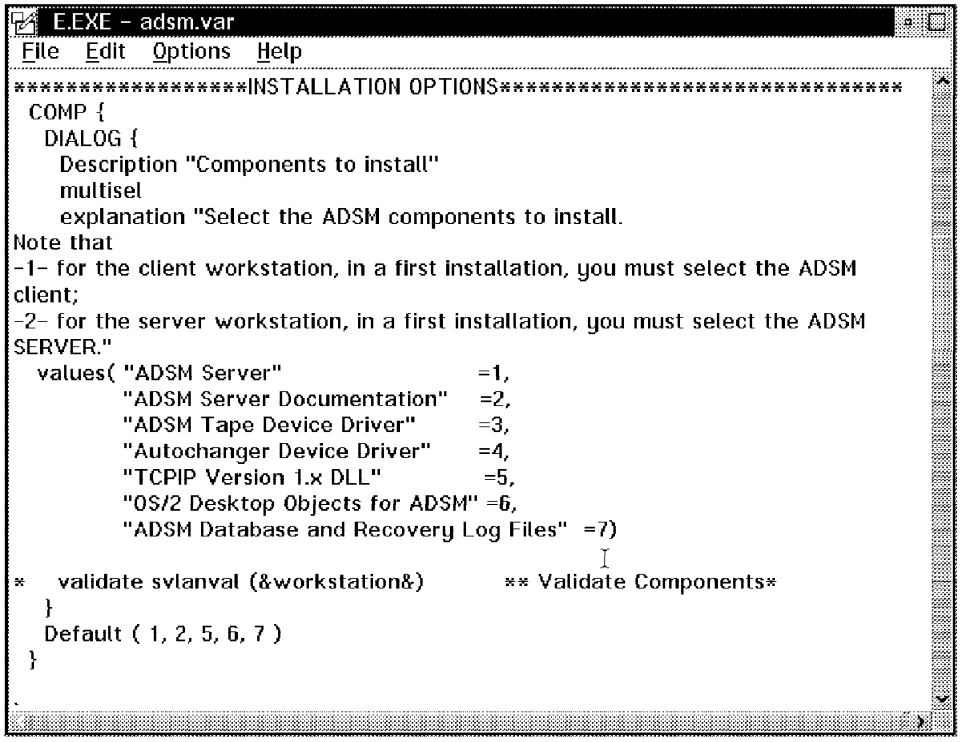


Figure 126. ADSM.VAR File Part 2 of 3

Finally the third part, Figure 127 on page 97, shows the values for the different installations options.

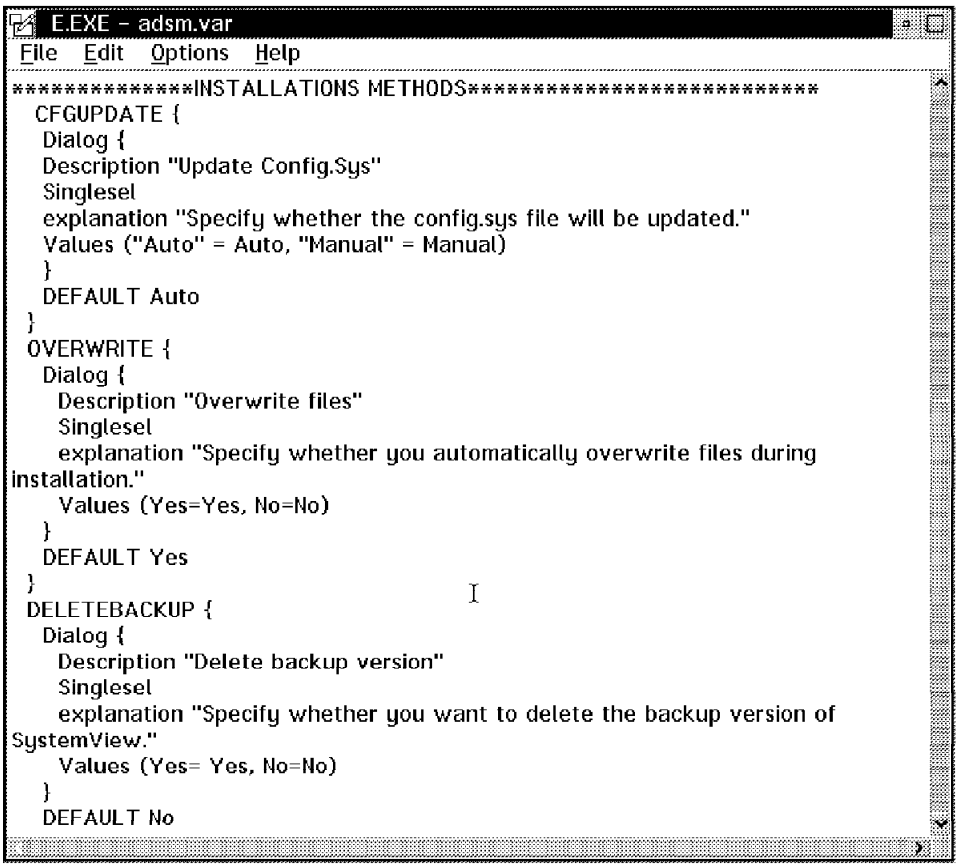


Figure 127. ADSM.VAR File Part 3 of 3

Note

The above three files should be stored in the following path:

* D:\SYSVIEW2\SWLIB

The next step is to catalog the software package. On the CID Software Preparation:

- Click on **Software Library**.
- From the menu bar click on **Software**.
- Click on **New**.
- Type a name and the file extension (ADF) you want to catalogue.
- Click on **Add**.
- An icon with the name you entered should appear in the same window.
- Double-click on it.
- The Software Configurations for ADSTAR Distributed Systems Manager should appear (or whatever name you chose).
- On this screen click on **Configuration** and then **New**.
- The CID Notebook with the name of your application should appear.
- Type the ID. It must be unique because it will be used to build the Global Name.

After going thorough the notebook to verify its contents (the information contained here is just a mix of the files ADSM.MCF, ADSM.VAR and ADSM.RSP), click on **OK.** You will get a pop-up window asking if the software package ADSTAR Distributed Systems Manager, should be cataloged. Click on OK and messages similar to Figure 128 and Figure 129 should appear. At this point the software package has been created and catalogued.

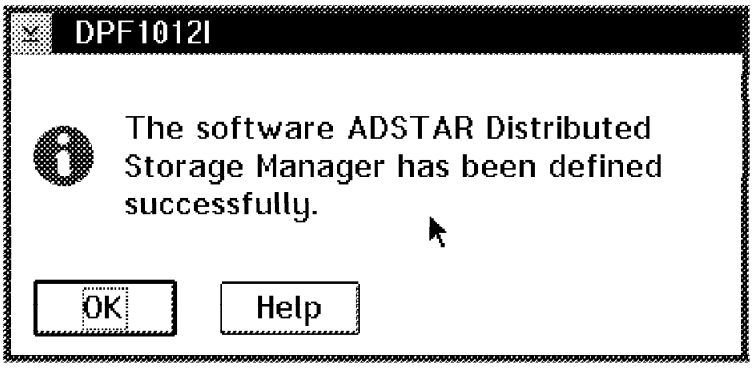


Figure 128. Successful Adding of ADSM Change File

A message about cataloging should appear immediately.

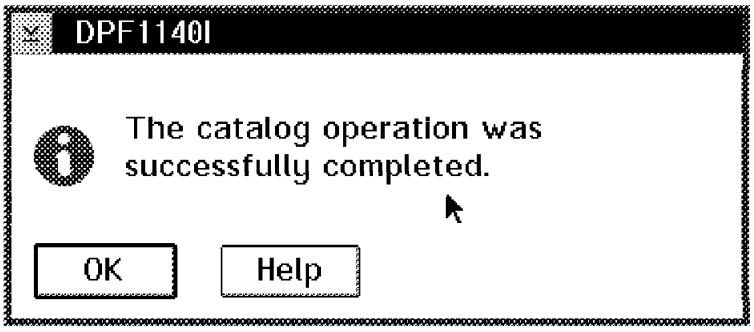


Figure 129. Successful Adding of ADSM Change File

Once you have created the change file and the response file models, the next step is to tie all the pieces together.

4.3 Software Inventory

This part shows the integration between:

- ADSM Code
- Inventory
- Genalert
- NVDM

The general idea is as follows:

- Schedule a software inventory check.
- Determine if the application that you want to distribute is already installed.

- If the application is not found, a generic alert will be triggered.
- A distribution process will start.

SystemView has the capability to discover software packages installed on remote systems. This is done through the use of dictionaries which contain most of the common applications found in the market. For our case, the application we want to discover is ADSM (ADSTAR Distributed Systems Manager). This application does not exist in the defaults dictionaries. Due to this, we had to add an extra item to the default dictionary. You will have two ways to create additional items. You can use a syslevel file which contains the specifications for the product you want to install. You can also add a new item to the search list that will be used in the exec when it does its pattern matching. In this case, we will be looking for DSMSERV.EXE. You can also provide the estimated size and the date of the executable module. Once you have added it successfully, you can to run an inventory on the system. The inventory can be stored in a flat file or just printed out. In this case the output of the inventory will be placed in a file. Figure 130 shows how to add a file to the list.

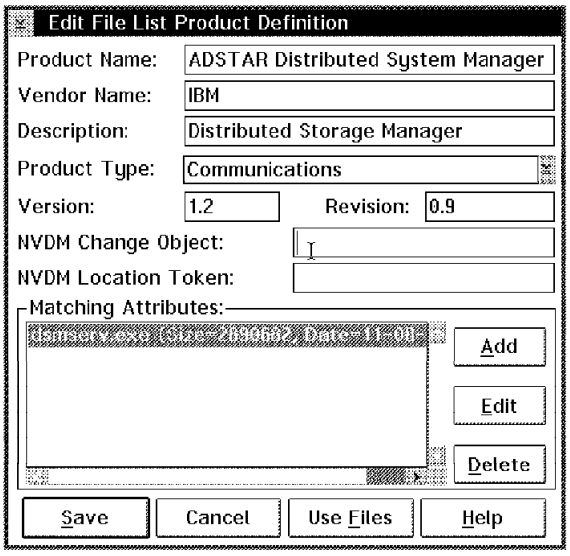


Figure 130. File Product Edition

Now the dictionary is ready to receive requests from the scheduler. The purpose of the scheduler is to run this inventory daily and record the information in a flat file.

The scheduler service should be configured as follows:

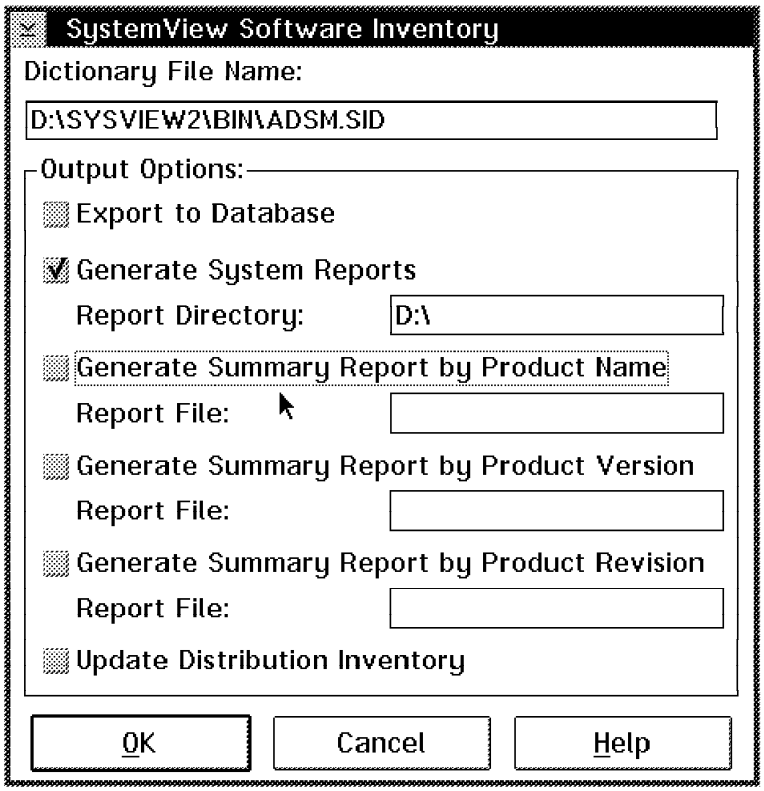


Figure 131. Scheduling Options

- Open the **Scheduler Service** icon on the NVDM Manager.
- Click on **New**.
- Assign a name for this event. We used ADSM.
- Click on the **Software Inventory task**.
- Click on **systems** and choose the **NVDM** client.
- Then select the **Schedule** option.

  Be aware that the name of the dictionary used should be the same that you updated earlier.
- Put the correct path for the reports. In this case it is D:-

  This path must be the same as the path that you will be specifying in the EXEC file (Figure 131).
- Click on **schedule**.
- In the next screen, just click on **daily**.

  The result should look like Figure 132 on page 101.

These steps will allow you to schedule a daily inventory for any selected target and search for any specific application. In this case, we searched for ADSM. The results of this searching will be stored in the file SVAUTAJ0.INV.

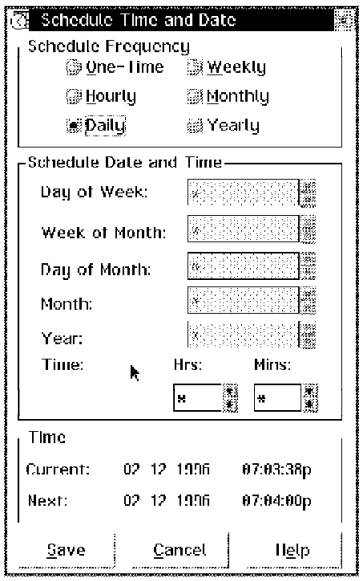


Figure 132. Timing

4.4 Evaluating Software Installed

In order to know whether the application is installed or not, we have to have our application parse the file that was created as a result of doing a software inventory. This was done using a simple REXX program. Figure 133 on page 102 shows the section of the program that was used to do the search.

The SysFileSearch is the key function. This internal function of REXX will allow us to search for a string in the file SVAUTAJ0.INV. If the word ADSM is located, the variable RES will be greater than zero and the program will send a message saying `The Product ADSM already exists in your machine`. The value of the string to search should be on of the words you typed in the product description and should be unique in all the files. Remember that this program was written as a simple sample to show you what can be done. You will probably write your own or just use this simple logic as your base.

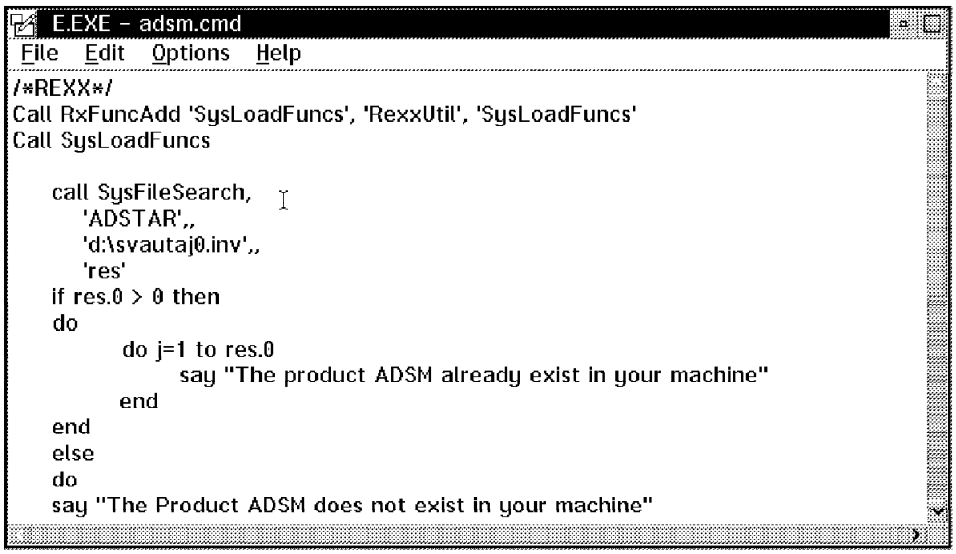


Figure 133. ADSM.CMD Section 1

4.5 Generating Alerts and Starting Distribution

The following part of the REXX command shows genalerts and the installation process. See Figure 134.

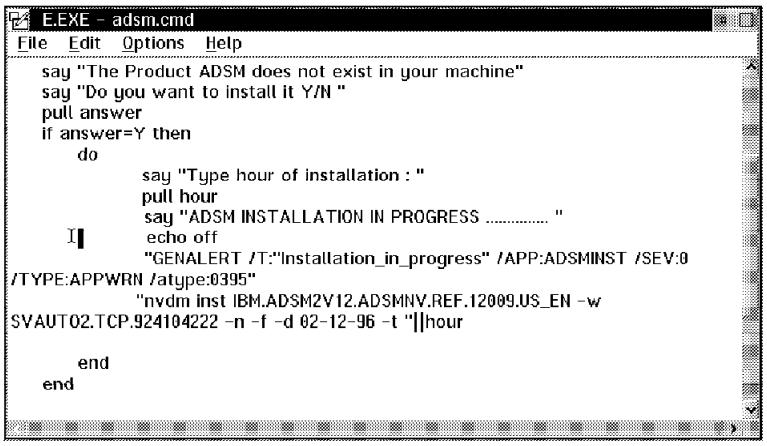


Figure 134. ADSM.CMD Section 2

If the application was not found, an alert message will be displayed in the OS/2 window saying `The Product ADSM does not exist in your machine. Do you want to install it Y/N.`

If you select **Y** an alert will be triggered with the characteristics showed in Figure 134. The format of genalert has already explained.

The next line is the NVDM command used to install the software package we created. The command is as follows:

```
nvdm inst IBM.ADSM2V12.ADSMNV.REF.12009.US_EN
      -w SVAUT02.TCP.92410422 -n -f -d 02-12-96 -t "]]hour
```

This line can be added here or even can be executed as a result of receiving an alert. We did not implement the second approach but rather the steps to do that follow:

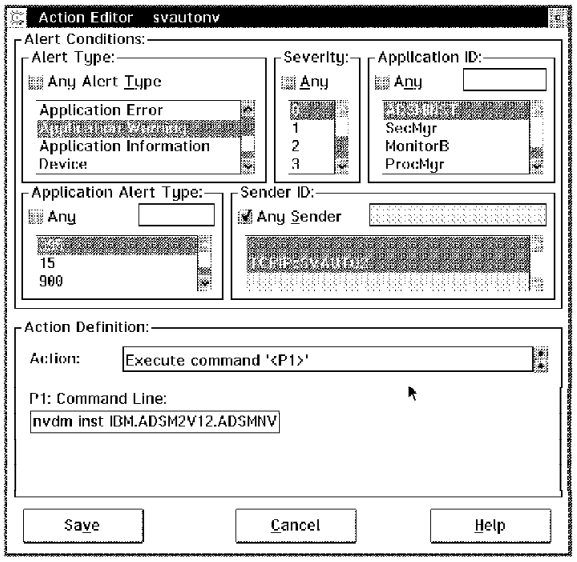


Figure 135. Action Editor

- Open your **SystemView Manager**.
- Click on the **Alert Manager** icon.
- Select **Actions**.
- Customize the parameters with the same values that you defined in the Genalert command. It should look like Figure 135.

The only difference is that the NVDM command is contained in the Action Editor.

The command Inst will take the change file defined for the global name IBM.ADSM2V12.ADSMNV.REF.12009.US_EN and will install it in the target defined by SVAUTO2.TCP.924104222. The next options are necessary in order to force the installation. The date should be written in the format mm-dd-yy and the hour hh:mm.

The results from this process follow:

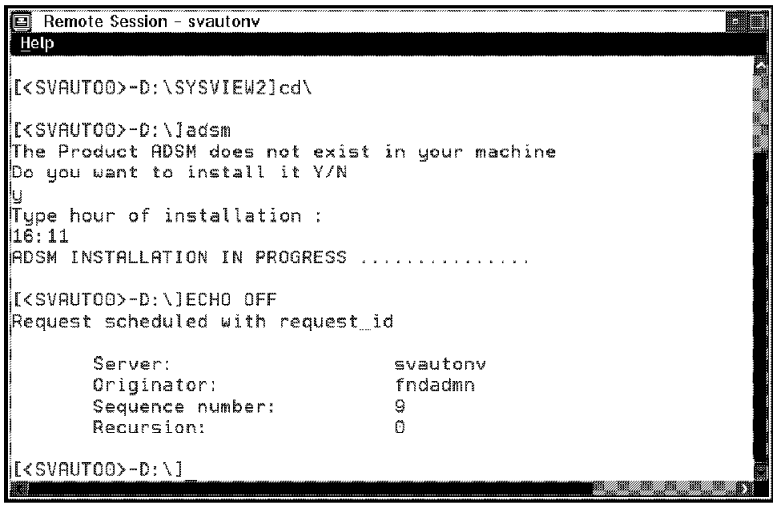


Figure 136. ADSM.CMD Execution

In the target machine, the status of the agent looks similar to Figure 137. At this stage, the process has been completed.

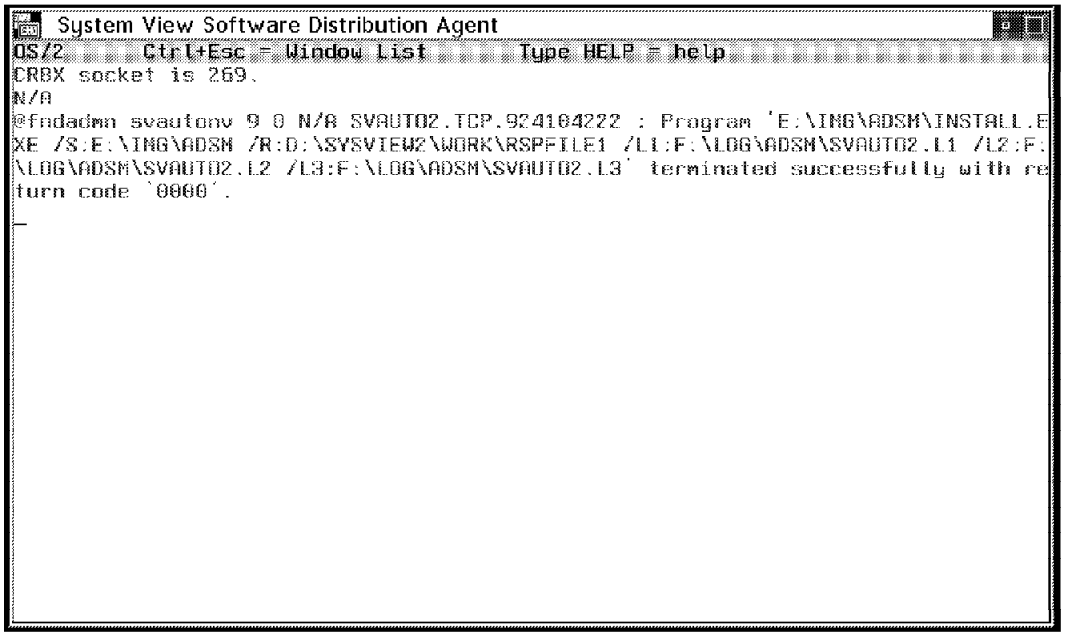


Figure 137. NVDM Agent Status

Finally, you can also review the process status by issuing the following command:

- `NVDM LSRQ #process -ou *`

  Here #process is the number NVDM gives you once the process has been submitted to a batch process.

The output should look like Figure 138 on page 105.

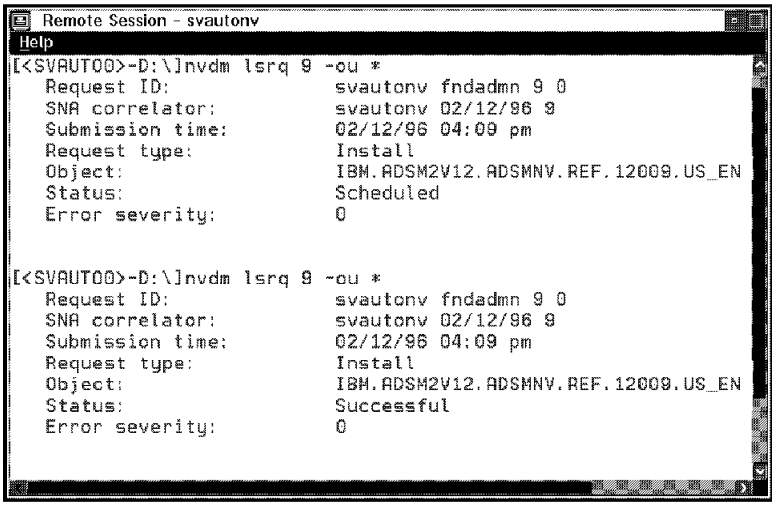


Figure 138. Distribution Process Status

Chapter 5. System Monitor

This chapter covers the wide set of System Monitors offered by SystemView for OS/2 on both the manager and client.

Note: The other monitoring capabilities of SystemView for OS/2, critical file monitoring and monitoring using remote workstation control, are not covered in this chapter.

The monitoring functions within SystemView for OS/2 and the actions that can be taken provide the building blocks for automation. Since there are many different monitors, and the thresholds can be set at any time by the manager, one can customize the automation for each of the resources that are monitored individually. The System Monitor function of SystemView for OS/2 helps to simplify these tasks. SystemView for OS/2 offers a rich set of monitors that are dependent upon the software and hardware that are installed on your workstation. Therefore, if you have not standardized on your hardware and software in your environment, it is likely that the set of available monitors differs from machine to machine. The person using the SystemView for OS/2 managing station will notice this as they start to use the Remote System Manager to look at the monitors available on the remote workstations.

There are many things to consider when you begin to implement a monitoring philosophy in your environment.

- Preventive Maintenance

  You can consider monitoring as a way to run your network in a pro-active way. This means that you can get early warnings of problems and resource shortages by setting your thresholds just below the problem point.

- Information Gathering

  Another consideration is information overload. If you monitor and capture data related to all of the monitors continually and never analyze that data, you will tie up extra resources. With SystemView for OS/2 you can set thresholds to cause specific actions to take place and therefore reduce some overhead of capturing data all the time.

- Interoperability

  SystemView for OS/2 can manage OS/2, Windows 3.1, Windows 95 and NetFinity NetWare clients. In addition, if you are using IBM Hardware for your PC Servers, you can obtain extended asset information. You can also interact with SystemView for MVS and SystemView for AIX.

- Integration

  You can even extend the scope of SystemView for OS/2s monitoring and its resulting actions by using REXX to run certain functionality of SystemView for OS/2 from the command line or launch it using REXX.

5.1 System Monitor Architecture

The architecture of SystemView for OS/2 is based on the separation of Base components and graphical user interface (GUI) components. The Base components gather information and makes it available to the GUI components. The GUI components read the information and formats it for viewing by the enduser. SystemView for OS/2 handles the exchanges between the Base and GUI components. You won't see a SystemView for OS/2 application that doesn't conform to this basic design.

- A GUI can be active without the matching Base component.

  This allows the SystemView for OS/2 managing workstation to run all available GUIs. There is no need to run the matching Base component on the same machine or anywhere else in the net.

- A Base can be active without the matching GUI component.

  This allows monitoring base to run and collect data without the need to start the monitoring GUI as well. There is no need to run the matching GUI component on the same machine or anywhere else in the network.

The communication is done either using the internal interprocess communication (IPC) of the local workstation or using the supported protocols (TCP/IP, IPX or NetBIOS).

5.1.1 Local Base - GUI Communication

If the Base and the GUI components of SystemView for OS/2 are running on the same machine the Base and GUI communicate using IPC as follows:

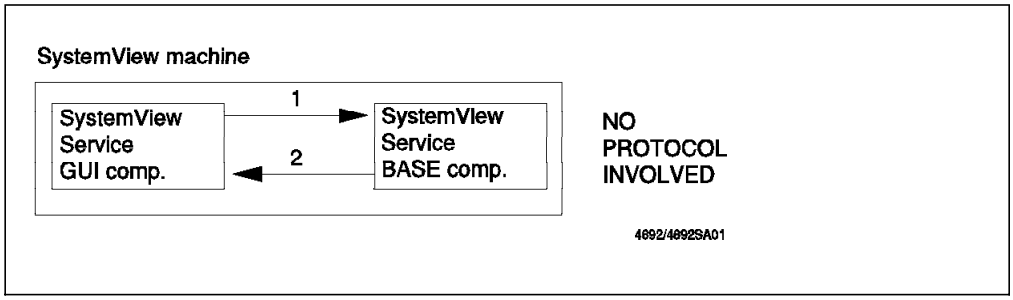


Figure 139. Local Base - GUI Communication

1. The GUI sends a message to the Base, which resides on the same machine.
2. The Base processes the message and returns the data to the GUI.

The implications of this are as follows:

- The monitoring Base (MONBASE.EXE) is started during the SystemView for OS/2's startup procedure.
- The Base gathers data continuously for every monitor available and stores data for every data recording-enabled monitor (please see 5.3.1, "The Monitors Pull-Down Menu" on page 120) in the MONDATA.INI file.
- If the GUI is started, it contacts the Base using IPC and requests the data it needs.
- As a result of this request, the Base returns the requested data using IPC.
- The GUI displays the data using the results of this query.

5.1.2 Remote Base - GUI Communication

If the Base component of SystemView for OS/2 is running on a remote machine, the Base and GUI communicate using the supported transport protocols. In addiition, a serial connection can be used.

SystemView for OS/2 supports the following protocols:

- NetBIOS
- IPX
- TCP/IP

Remote communication between Base and GUI can be shown as follows:

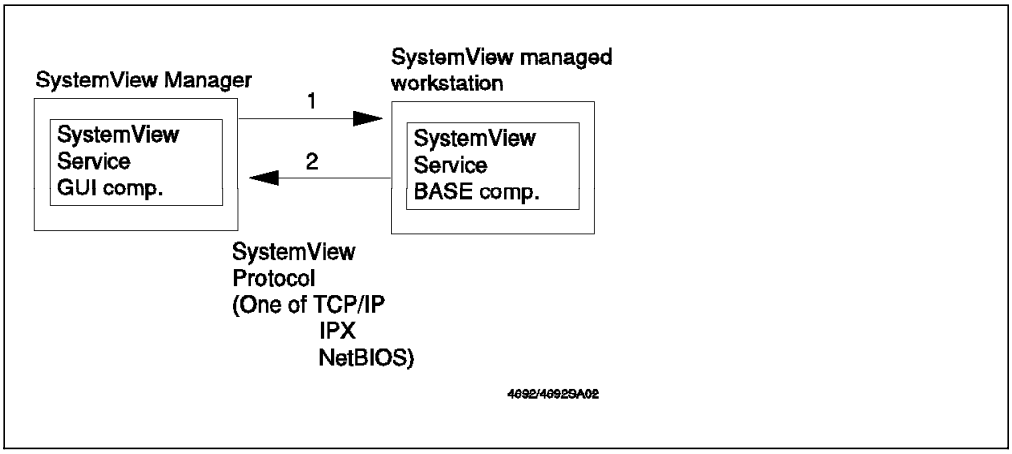


Figure 140. Remote Base - GUI Communication

The communication between the Base process and the GUI works as follows:

1. The GUI sends a message to the remote Base.

   The GUI communicates with the Base using NetBIOS, IPX, TCP/IP or the serial connection.

2. The Base processes the message on the remote machine and returns the data to the GUI using one of the previously mentioned options.

What this means is the following:

- The monitoring Base (MONBASE.EXE) is started during the SystemView for OS/2′s startup procedure on the client workstation.
- The Base gathers data continuously for every monitor available and stores data for every data recording-enabled monitor (please see 5.3.1, “The Monitors Pull-Down Menu” on page 120) in the MONDATA.INI file. It doesn′t matter if the monitor was started locally or from a remote manager.
- If the GUI, located at the SystemView for OS/2 managing machine, is started, it contacts the Base using one of the previously mentioned ways and requests the data it needs.
- As a result of this request, the Base returns the requested data using the specified method (NetBIOS, IPX, TCP/IP or serial).
- The GUI builds the monitors using the results of this query.

Note: The GUI and Base functional exchange works the same way whether or not they are on the same machine. The only difference is how the data exchange between the Base and GUI is handled.

5.1.3 Special Case of Base - GUI Communication

The only part of SystemView for OS/2 which doesn't completely follow the communication described in 5.1.1, "Local Base - GUI Communication" on page 108 or 5.1.2, "Remote Base - GUI Communication" on page 109 is the event scheduler.

Event scheduler

Please note that only SystemView for OS/2 managing workstations have the Event Scheduling option.

The Base component of the event scheduler talks to the GUI component of the event scheduler in the same way as the Base would.

- If you schedule events using your local event scheduler Base component, the event scheduler's Base - GUI communication is done using IPC (please see 5.1.1, "Local Base - GUI Communication" on page 108).
- If you schedule events using another SystemView for OS/2 manager's event scheduler Base component, the event scheduler's Base - GUI communication is done using a communication protocol or the serial communication (please see 5.1.2, "Remote Base - GUI Communication" on page 109).

The difference is:

- The scheduled event is *always* processed using the protocols or using the serial connection capability of SystemView for OS/2.
- Even if the event is scheduled for the local machine, SystemView for OS/2 will not use IPC to do the connection but the protocol which has been defined while setting up the event.

The communication used by the event scheduler is shown in the following two figures:

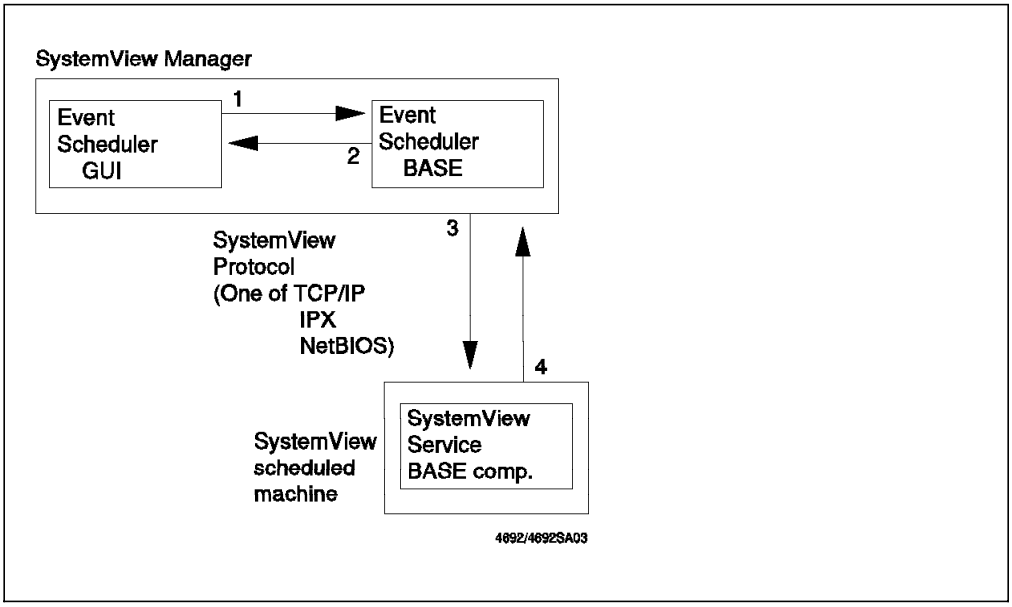


Figure 141. Event Scheduling Comm - (Scheduler Base and GUI on One Workstation)

The communication works as follows:

1. The GUI sends a message to the Base, which resides on the same machine, using IPC.
2. The Base processes the message and returns the data to the GUI using IPC.
3. The Base processes the scheduled event using the defined protocol or the serial connection.
4. The Target communicates the result of the scheduled operation using the defined protocol or the serial connection.

Note: Please note that the communication for the scheduled event (Steps 3 and 4) is *always* done using the defined Protocol or the serial connection even if the target is the local.

The execution of a scheduled event is never done using the IPC machine.

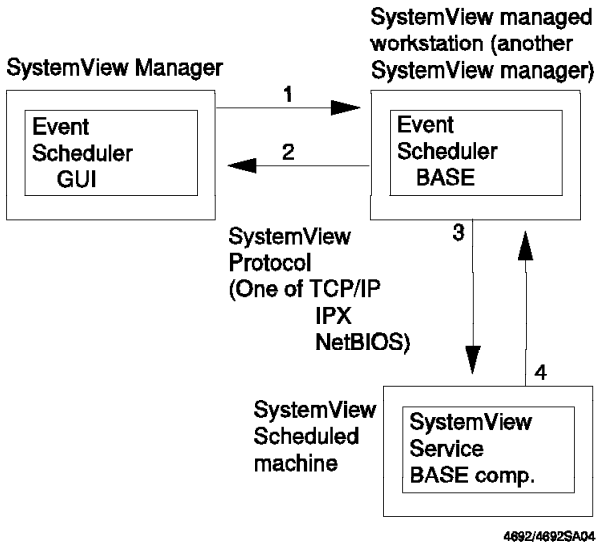


Figure 142. Event Scheduling Comm - (Scheduler Base and GUI Separate Workstations)

The communication works as follows:

1. The GUI sends a message to the Base, which resides on another SystemView for OS/2 managing workstation using the defined protocol or the serial connection.
2. The Base processes the message and returns the data to the GUI of the calling SystemView for OS/2 managing workstation using the defined protocol or the serial connection.
3. The Base processes the scheduled event using the defined protocol or the serial connection.
4. The Target communicates the result of the scheduled operation using the defined protocol or the serial connection.

Note: The communication for the scheduled event (Steps 3 and 4) is always done using the defined Protocol or the serial connection even if the target is the local machine. The execution of a scheduled event is never done using IPC.

5.2 System Monitor Service

The process of gathering and processing information for the system monitor starts when SystemView for OS/2 is started. SystemView for OS/2 starts many programs during startup. One of these is the base process for monitoring:

MONBASE.EXE

This process captures all of the monitoring data for the monitors that are configured for this machine. The presentation is done using the System Monitor GUI:

MONGUI.EXE

All of the data that is related to the monitoring process is stored in INI files. The data that we are referring to is configuration and collection data.

MONGUI.INI Contains the layout of all of the System Monitors for this machine
MONTHR.INI Contains the threshold definitions for this machine
MONSCH.INI Contains the available monitors for this machine
MONDATA.INI Contains the data collected by the Base

The size of MONDATA.INI depends on the number of monitors which are activated for data recording, on the period of time they are active and on the settings you made for the monitors.

You activate the System Monitor GUI by double clicking on the System Monitor template, or by starting MONGUI.EXE.

Note: If you want to access the System Monitor on remote machines, you must first use the Remote System Manager to connect to the remote machine.

The name of the remote machine is always displayed in the title bar of the window or pop-up opened.

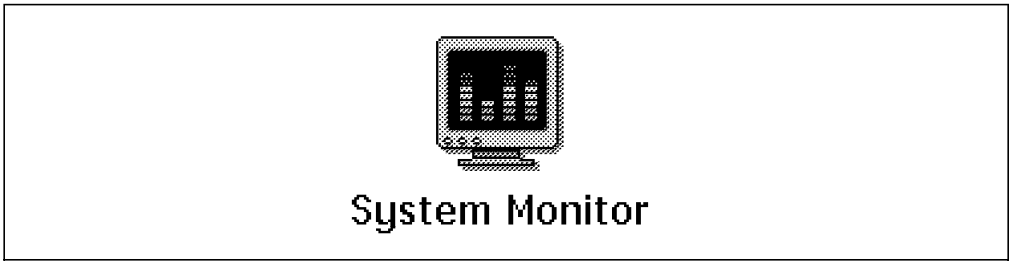


Figure 143. System Monitor Template

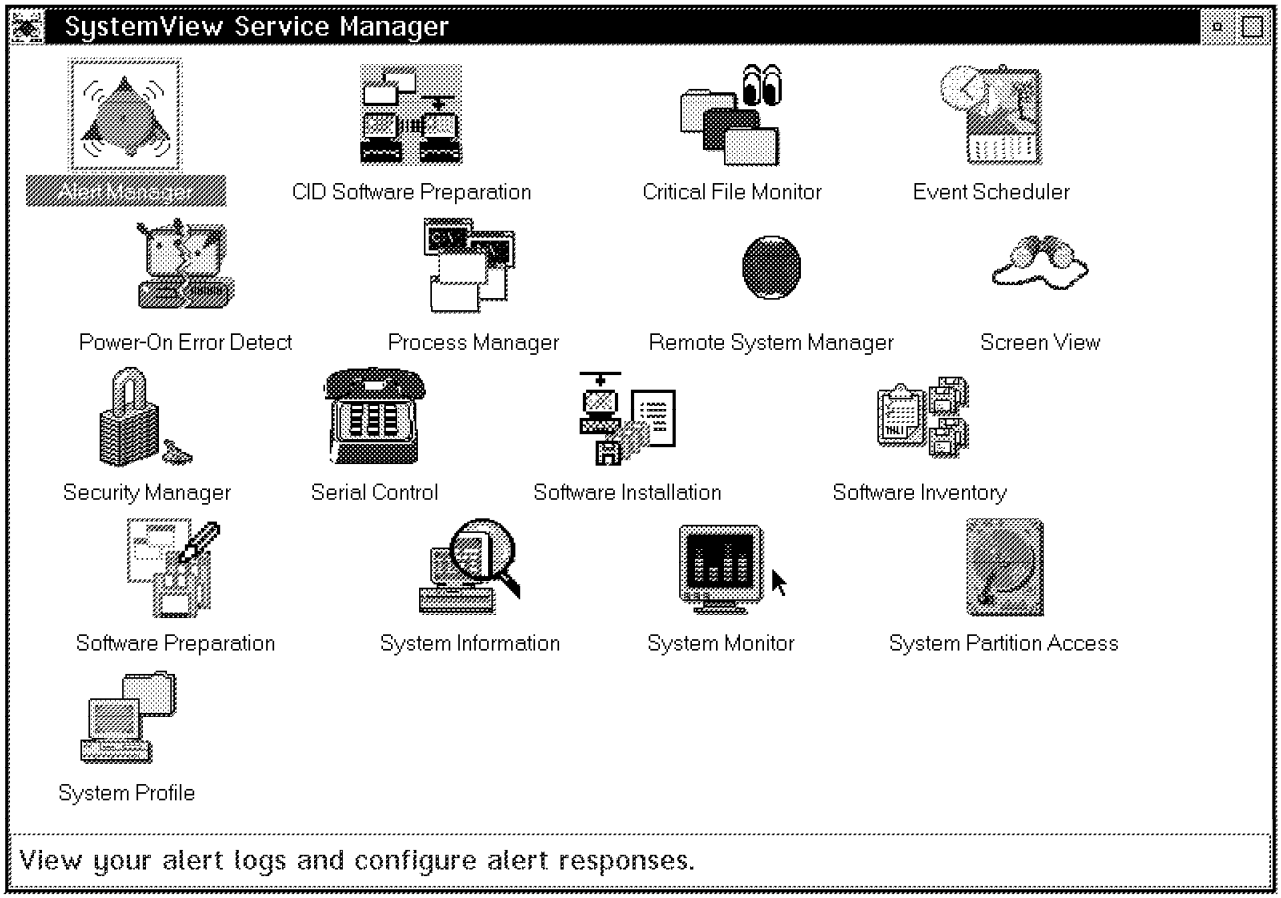


Figure 144. SystemView Service Manager - System Monitor

Double-click on the **System Monitor** symbol in the Service Manager window and the System Monitor Service window appears as shown below:

Figure 145. SystemView Service Manager

After the System Monitor Service window appears, all of the monitors that have been configured to be operational from a GUI perspective will appear on the screen. The default monitor on most machines is the CPU Utilization monitor. This is true of most, but not all systems. On ThinkPads, the status of the battery is the default monitor that is displayed. The default display for all of the monitors is to not have an action bar or a title bar on them. In order to add it, you will need to use the right-mouse button within the window to configure it.

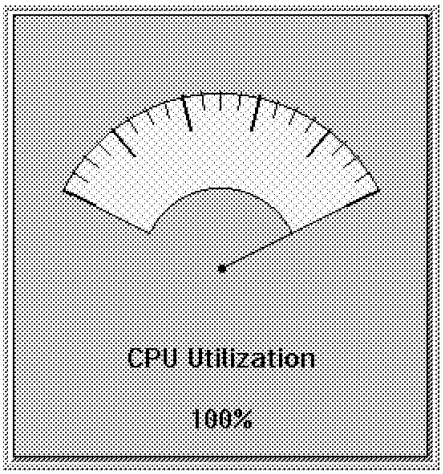


Figure 146. CPU Utilization

If you access a remote workstation, the title bar of the remote workstation is always displayed by default:

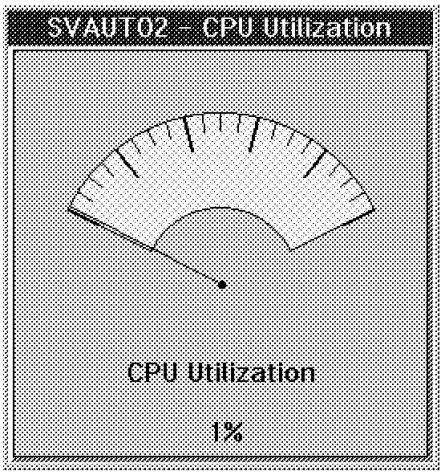


Figure 147. CPU Utilization - Remote Workstation

The action bar of the System Monitor Service window has the selections Windows and Help. Selecting Help brings up the SystemView Help facility. This document does not cover the Help facility.

Click on **Windows**.

The Windows pull-down appears with the following choices:

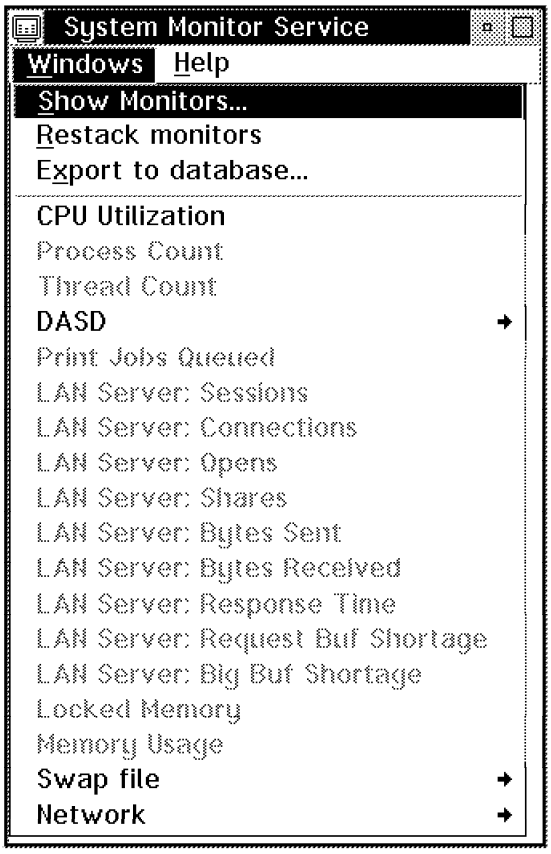


Figure 148. System Monitor Service - Windows Pull-down

The pull-down is divided into two sections:

1. The first section is where the actions can be defined.

   This section offers the following choices:

Show Monitors	Click here for the Select Visible Monitors pop-up window. Please see 5.2.1, “Select Visible Monitors” on page 119.
Restack Monitors	If you have overloaded your display by displaying too many monitors at the same time, you can easily reorder them. An example of having many monitors spread across the display is shown in Figure 149 on page 117.

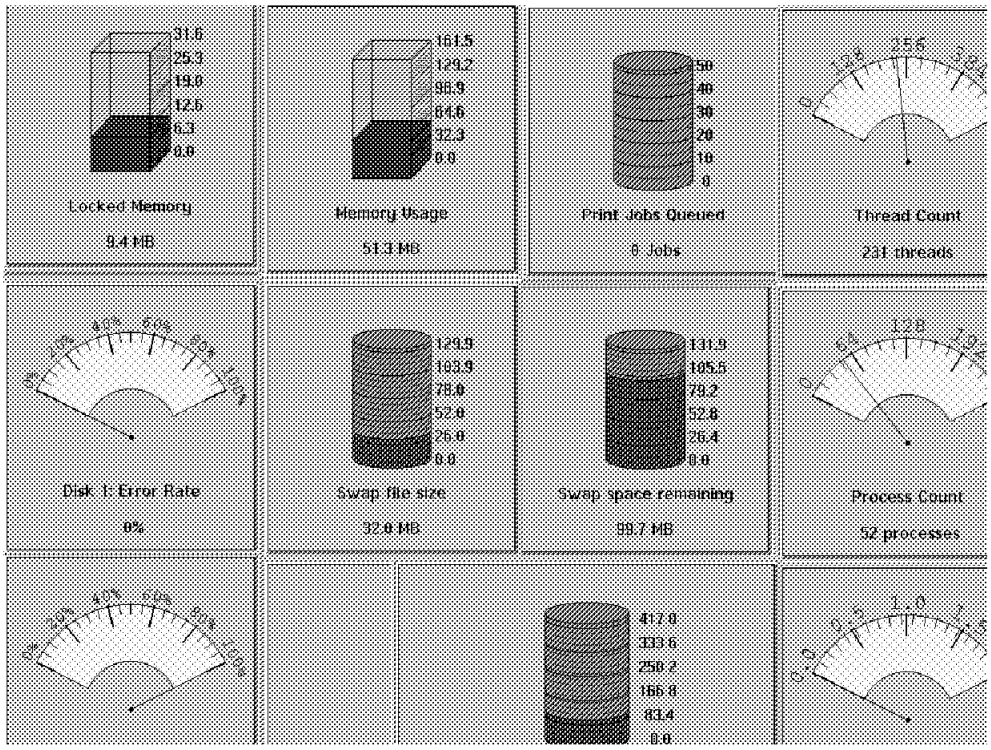


Figure 149. Too Many Monitors on the Display

You simply need to click on **Restack** Monitors to clean up the display.

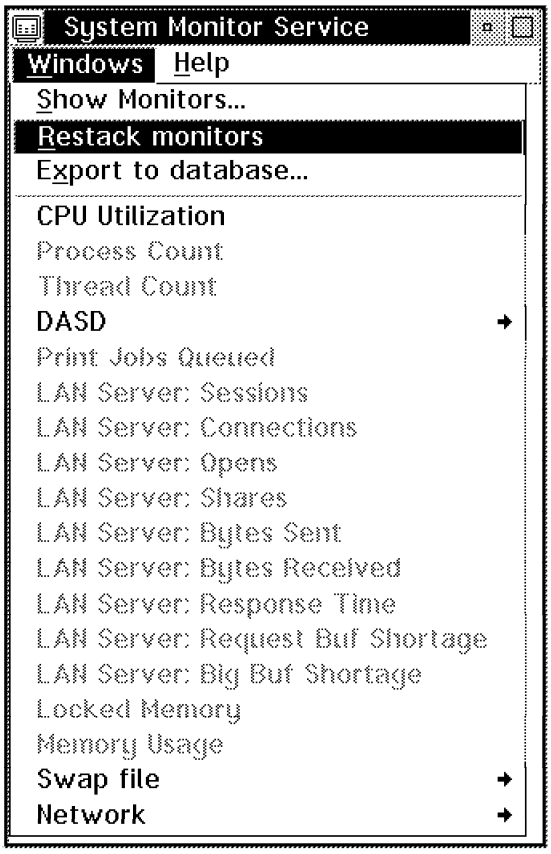


Figure 150. Restack Monitors Selection

After you restack the monitors, they will appear as follows:

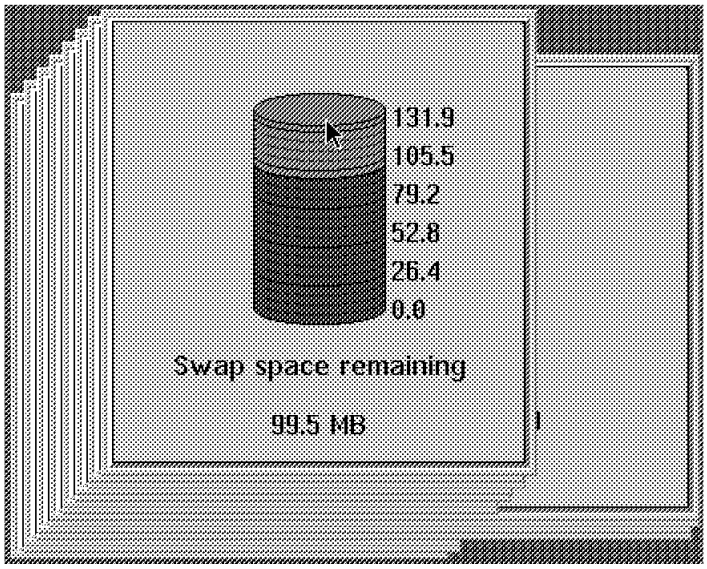


Figure 151. Restacked Monitors

Export to Database Click here to initiate the export of the monitoring data to the database (DB 2 /2, or Lotus Notes database).

Please see 5.2.2, “Database Entry Selection” on page 119 for details.

2. The second part of the screen determines which monitors will be actively displayed on the GUI. If the monitor had been previously selected, but for some reason it couldn′t report on its data, it will still appear on the display, but it will appear as a faded symbol.

   Some of the monitors are clustered in the menu, and in order to activate them, you need to click on the arrow within the list.

5.2.1 Select Visible Monitors

The Select Visible Monitors Pop-up shows a list of all available monitors for this the computer. The visible monitors are highlighted. To make the monitors visible, simply click on the monitors you want to appear on the desk top and then click on **Accept**.

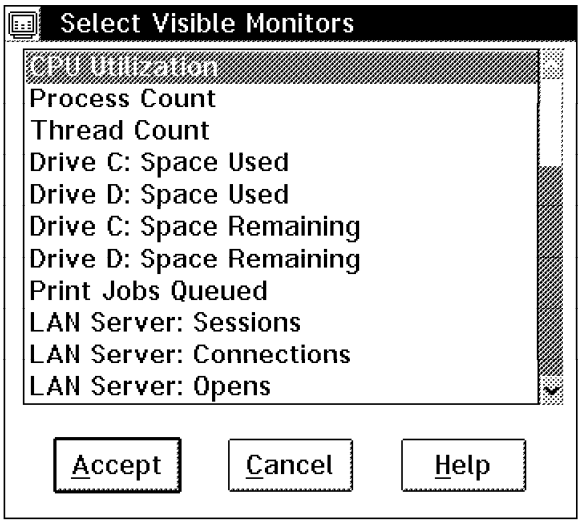


Figure 152. Select Visible Monitors

SystemView for OS/2 will immediately display the selected monitors on the screen.

5.2.2 Database Entry Selection

The Database entry selection pop-up gives you a list of all installed databases and lets you select which database you prefer to store the data recorded by the System Monitor function.

Note: The data recorded here has no relation to the data used by MONGUI.EXE to do the graphical interpretation on screen. The customization of values for database storage is just a tool for you to store the data in a way that you can use the database in a convenient way.

The selection made here is a general selection. It can be overwritten for every single monitor. Just click on the monitor using the right mouse button and then click on **Export** to database in the pull-down menu. If you access the Database entry selection pop-up from the monitor, you can only change the value for the currently accessed monitor. If you call it from the Windows pull-down of the

System Monitor Service Window, you can assign the preferred database for each monitor available on this machine. In addition, you can only initiate database records for monitors that are not being displayed using this process.

The Database entry selection pop-up appears as follows:

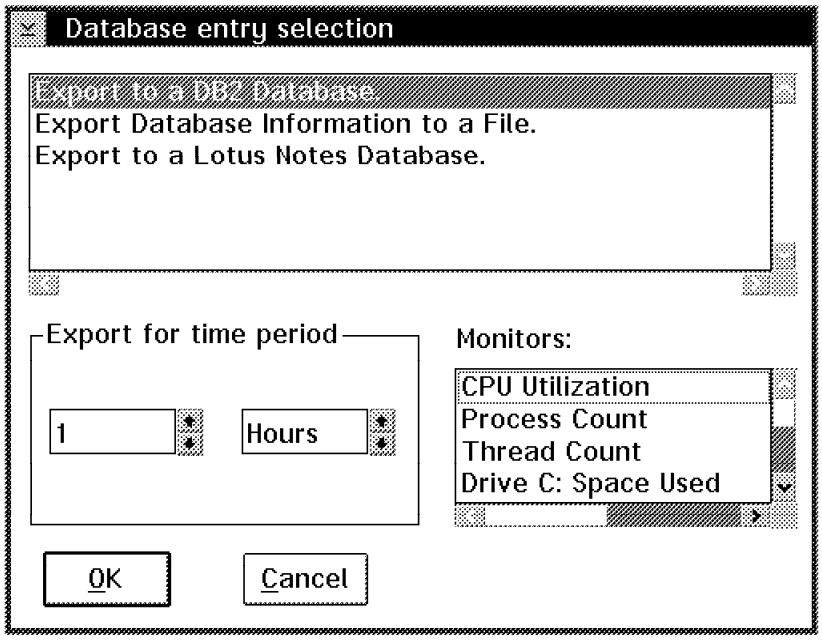


Figure 153. Database Entry Selection

5.3 Customization of Monitors

SystemView for OS/2 offers three different layouts to display its monitors:

- Real Time

  In the real time window, you can see the last captured value displayed.

- Line Graph

  In the line graph layout you see a graph, which shows the deltas of the captured values within a given timeframe.

  The line graph is only available if data is beint actively recorded for this monitor.

- Text display

  In the text display window you see the last captured value for the related monitor. The only difference with the real time display is the graphical representation. The values are exactly the same.

5.3.1 The Monitors Pull-Down Menu

Every monitor has a notebook attached where the monitor can be customized.

You can activate a pull-down, which gives you the choices for each monitor by clicking on that monitor using the right mouse button. The pull-down looks as follows:

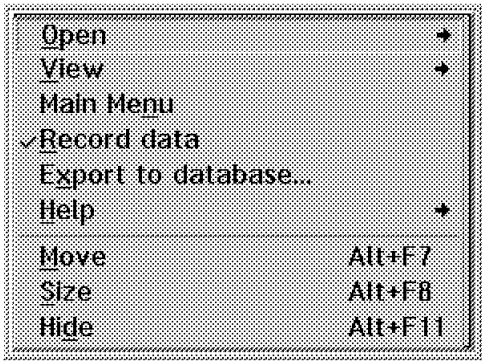


Figure 154. A System Monitor's Pull-Down Menu

This pull-down offers the following entries:

Open →
: Open the monitor's attached notebook.

  You can select to open the threshold or the setting section of the notebook.

View →
: Change the layout of the monitor.

  You can choose between one of the following:

  - Line graph
  - Real time
  - Text display

Main Menu
: Switch immediately to the System Monitor Service window.

Record data
: Check to activate data recording for this monitor.

  Record Data Off

  If *Record data* is off, the Line graph layout is deactivated.

  If you stop recording, all data for the line graph layout for this monitor is lost. Changing Record data to off causes the deletion of the referenced data in MONDATA.INI immediately. Turning it back on does not get the data back. The data gets stored for post-processing. SystemView for OS/2 doesn't retrieve any data from the database, it only puts the data there.

Export to database...
: See 5.2.2, "Database Entry Selection" on page 119 for an explanation of this field.

Help
: To invoke the help facility.

Move
: Move the monitor to another place on the display.

Size
: Change the size of the monitor.

Hide
: Hide the monitor.

  This selection removes the monitor from the screen. It also removes the monitor from the visible monitor list of the System Monitor Service's Windows pull-down.

5.3.2 Monitor Notebook

Every monitor has a notebook associated with it where you can store customized values for each monitor. The notebook consists of two pages. The name of the notebook is based upon the monitor being customized.

5.3.2.1 The Monitors Notebook Settings

Page one of the notebook contains the general customization:

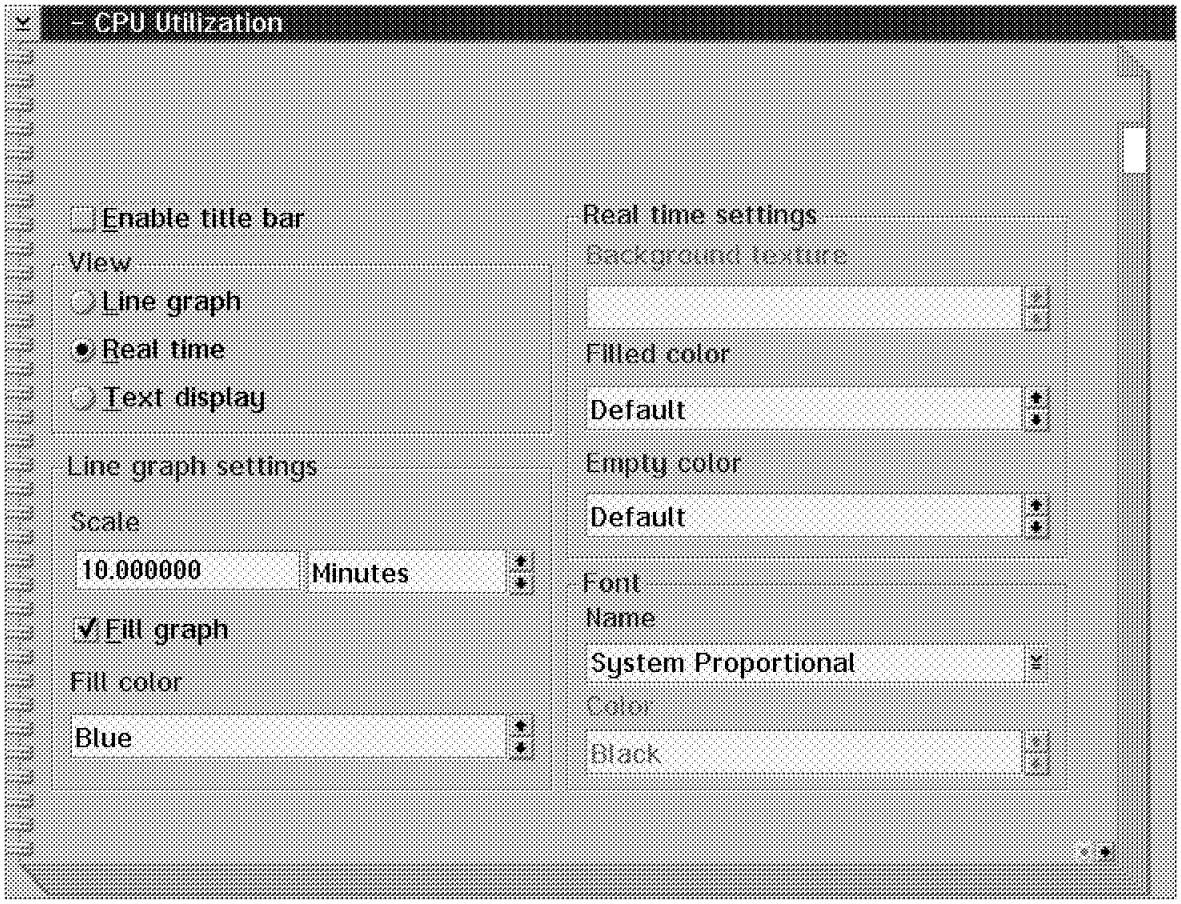


Figure 155. Settings for a System Monitor Notebook

You can change the following:

Enable title bar — Checkbox.

Select whether a title bar for the monitor is to be displayed.

Title Bar

The default setting for the title bar on a local monitor is off.

The default setting for the title bar on a remote monitor is on.

The defaults make it easy to identify which machine's monitor you have on the display.

View	Select whether the monitor is to be displayed in: • Line graph • Real time • Text display
Line graph settings	Here you can customize the line graph layout. You can change the scaling. You can decide if the graph is to be filled in or only displayed as a line. If the graph is filled in, you can select the color to be used.
Real time settings	Here you can customize the line Real time display. You can: • Change the background texture (where available). • Change the filled color of the real time layout. • Change the empty color of the real time layout.
Font	Here you control the font used regardless of the layout.

5.3.2.2 The Monitors Notebook Thresholds

Page two of the notebook contains the Threshold settings as follows:

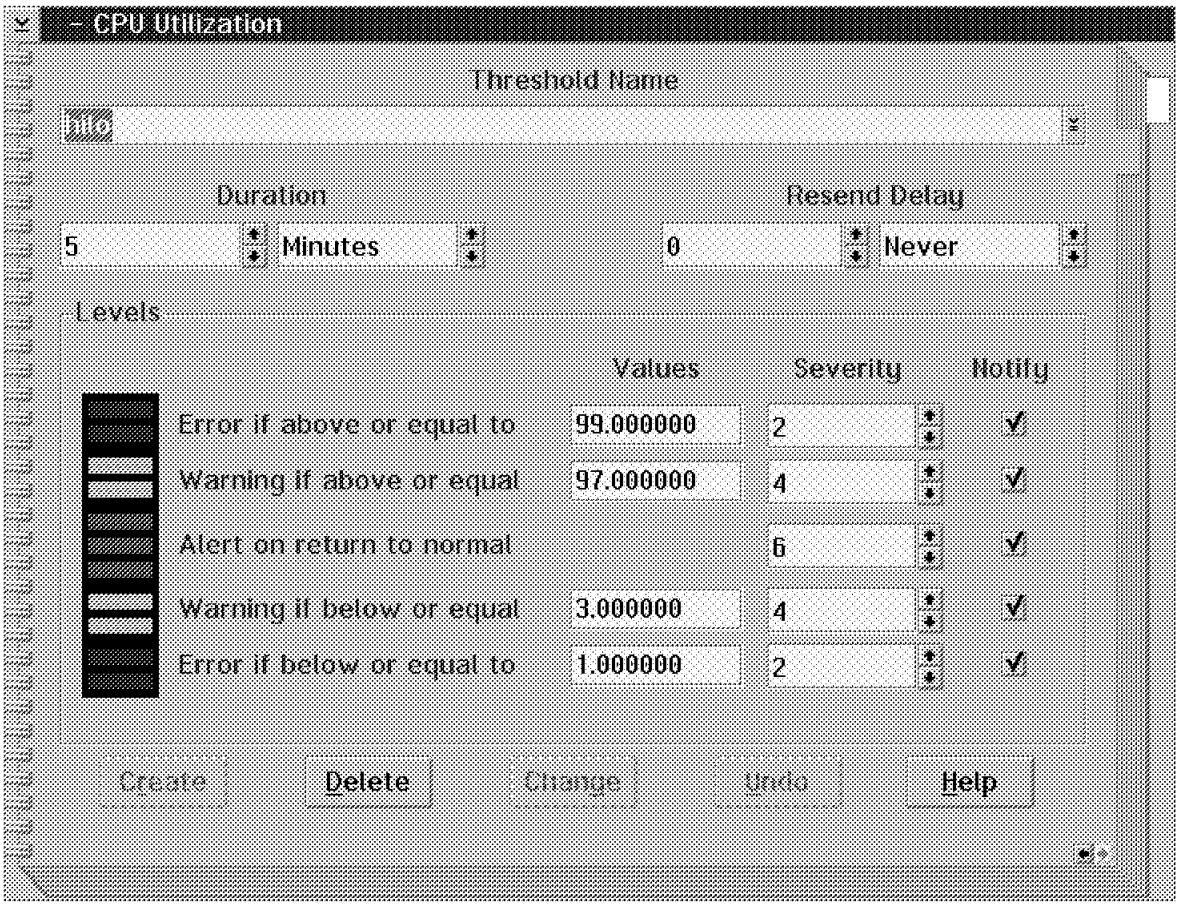


Figure 156. Thresholds for a System Monitor's Notebook

Here you can generate system monitor alerts depending on the threshold defined. You can forward the alerts in the network to a manager using SystemView for OS/2's Alert Manger.

If you access the notebook of a remote machine, it looks slightly different:

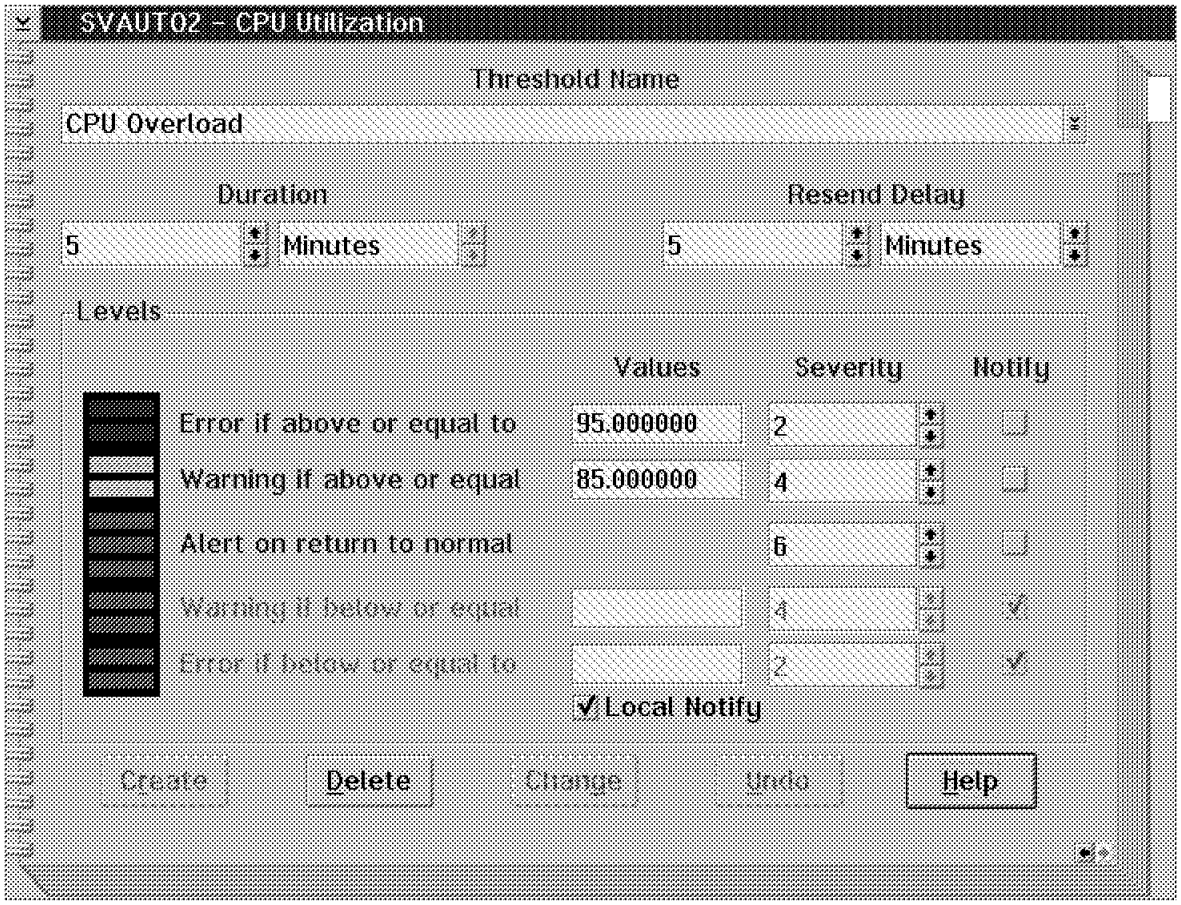


Figure 157. Thresholds for a System Monitor's Notebook - Accessed Remotely

Please note the Local Notify checkbox. at the bottom of the notebook. Here you can specify if the threshold set by you for the remote machine generates an alarm at the local machine as well as forwarding it onto the manager.

Keep in mind, that SystemView for OS/2 follows the Base - GUI guideline. If you change thresholds on remote machines, the MONTHR.INI file is changed on the remote machine. The user at the remote machine can override your settings using his local System Monitor application.

If you are already connected to the remote machine, you will not receive any notification for this change. Your pop-up will not be refreshed either and you will think, that everything is set up as you did it. To assure that the contents of the remote monitor's pop-up is up-to-date, you must stop the remote connection and reconnect again.

5.4 Available Monitors

The monitoring section of SystemView for OS/2 contains some problems you should be aware of if you use it.

- Some monitors have a sizing problem. The default size of the monitor does not allow you to display the monitor's name.

- If you don′t see the monitor′s name in the original layout, re-size it until it is displayed.
- In its default form, sometimes the longitude′s values are not completely displayed. You must re-size the monitor to make it wider to solve this problem.
- All monitors appear on the workplace shell of OS/2.

  If you have many monitors active, this results in a screen full of monitors, thus confusing the operator To solve this problem, you will have to restack the monitors, do a manual restack or gather data for the monitor but hide it and look to it from time to time.
- If you restack the monitors, SystemView for OS/2 restacks them in the default form and size. All customization regarding size and form of the monitors is lost.
- If you stop and restart the monitors, the monitors appear in their default form and size. All customization regarding size and form of the monitors is lost.

5.5 Common OS/2 Workstation-Oriented Monitors

The following sections show monitors that will be on all OS/2 workstations. While SystemView for OS/2 supports many different monitors, and the ones that appear in your System Monitor service window are dependent upon what facilities are on your system, the following will be on all OS/2 systems:

- CPU Utilization
- Process Count
- Thread Count
- Drive Space Used
- Drive Space Remaining
- Print Jobs Queued
- Locked Memory
- Memory Usage
- Swap File Size
- Swap Space Remaining
- Disk Workload
- Disk Error Rate

5.5.1 CPU Utilization

The CPU Utilization monitor shows the current workload on the CPU, as a percentage of its maximum capacity. A meaningful use of the thresholds setting capability of SystemView for OS/2 can help you to determine which machines are busy in your network and which are not. Sometimes it′s helpful to move some applications from busy machines to other ones to solve this kind of capacity problem.

It is also possible to send SNMP traps to an SNMP manager like NetView for AIX and use its correlation engine to see if multiple monitors for the same workstation are exceeding thresholds. This may help in the capacity planning methodology.

The three possible views of the CPU Utilization monitor follow:

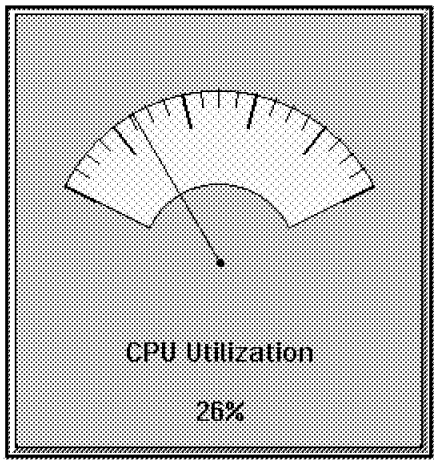


Figure 158. CPU Utilization Monitor - Real Time

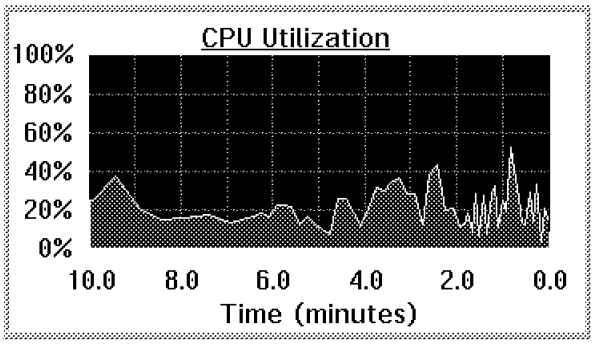


Figure 159. CPU Utilization Monitor - Line Graph

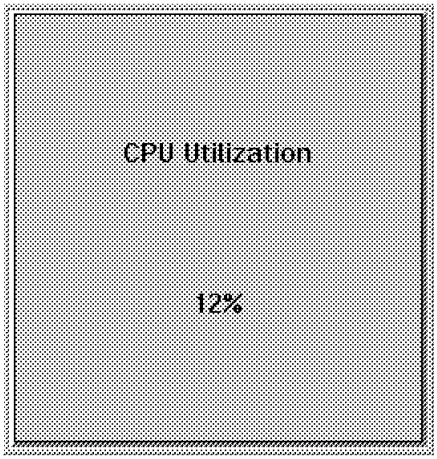


Figure 160. CPU Utilization Monitor - Text Display

5.5.2 Process Count

The Process Count monitor shows the number of active processes running concurrently on this machine. If the number of concurrently active processes tends to be too high, you might consider moving some workload from this machine to another one. A meaningful use of the thresholds setting capability of SystemView for OS/2 can help you to determine which machines are running too many processes and which are being under utilized.

The Process Count monitors are shown below:

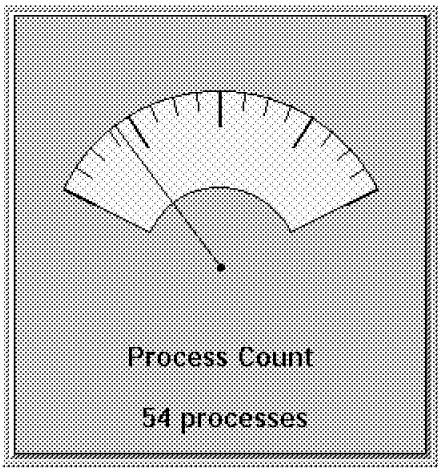


Figure 161. Process Count Monitor - Real Time

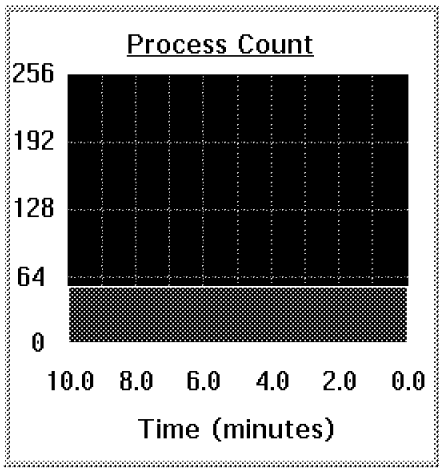


Figure 162. Process Count Monitor - Line Graph

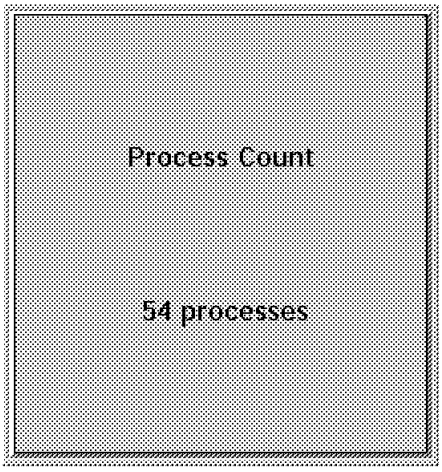


Figure 163. Process Count Monitor - Text Display

5.5.3 Thread Count

The Thread Count monitor shows the number of active threads running concurrently on this machine. If the number of concurrently active threads appears to be too high, (which means they are about to reach the limit defined in the THREADS statement in CONFIG.SYS) you should consider changing the CONFIG.SYS or to move some workload from this machine to another one. A meaningful use of the thresholds setting capability of SystemView for OS/2 is to help you to determine which machines are running close to their threads limit and which machines may be under utilized.

The Thread Count monitors follow:

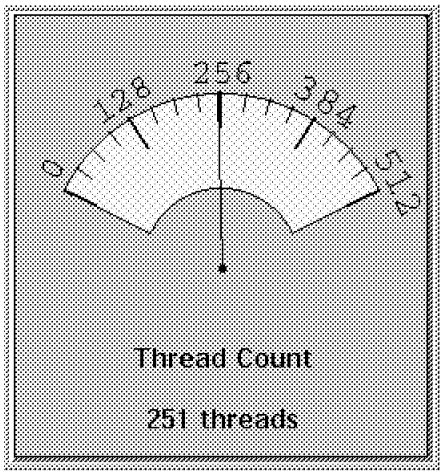


Figure 164. Thread Count Monitor - Real Time

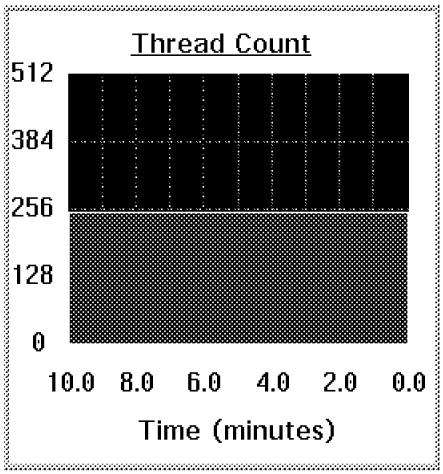


Figure 165. Thread Count Monitor - Line Graph

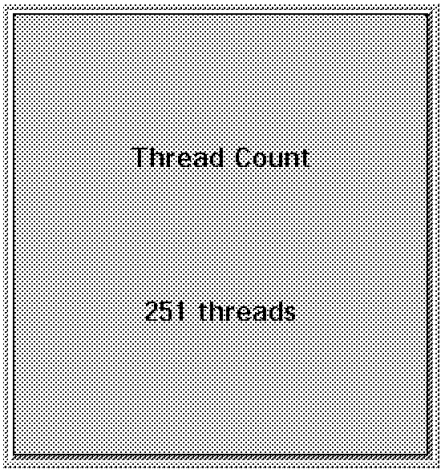


Figure 166. Thread Count Monitor - Text Display

5.5.4 Drive Space Used

The Drive Space Used monitor shows the space used for a drive for this machine. If the space threshold comes close to the space available, you should consider checking the hard disk to see if you can delete some files to get some space back or you could insert a new hard disk drive to get some more disk space. A meaningful use of the thresholds setting capability of SystemView for OS/2 can help you to determine which machines are running out of disk space and which are not.

From an automation perspective, it might be an opportunity to delete old files and directories that you know can be deleted.

The Drive Space Used monitors follow:

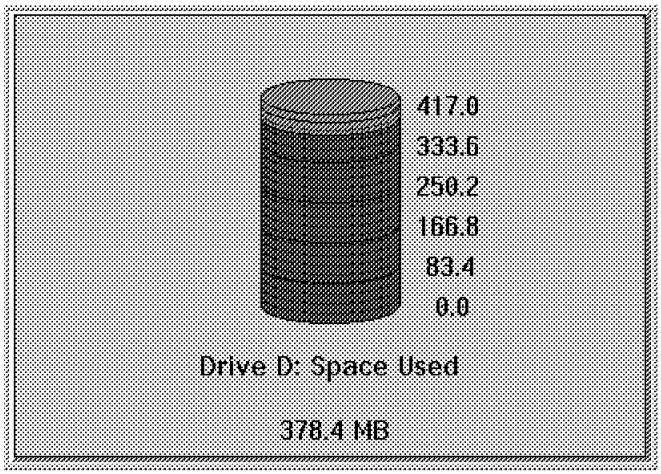


Figure 167. Drive Space Used Monitor - Real Time

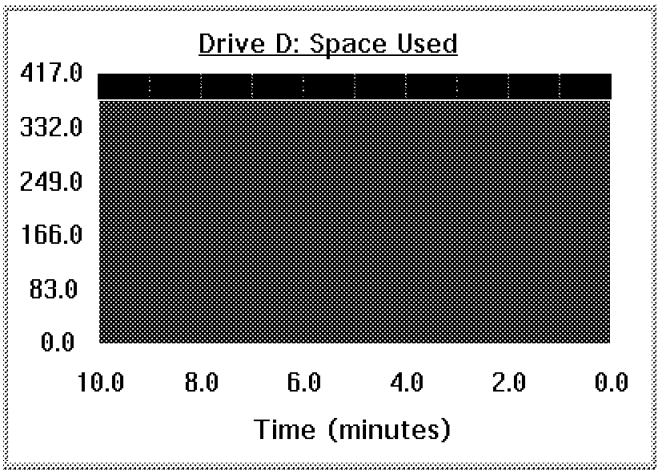


Figure 168. Drive Space Used Monitor - Line Graph

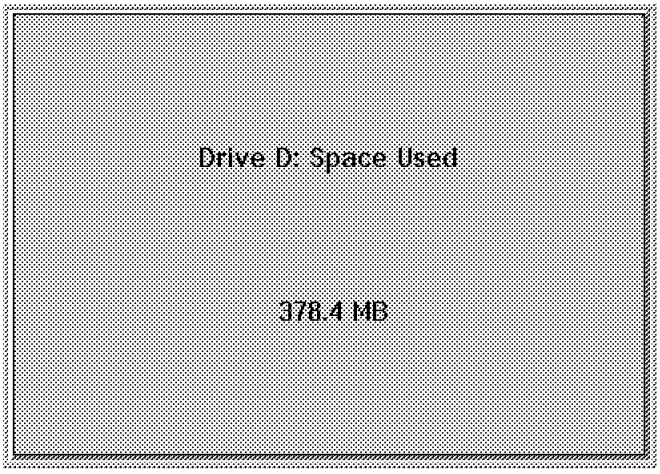


Figure 169. Drive Space Used Monitor - Text Display

Note: Every active hard disk drive has its own Drive Space Used monitor.

5.5.5 Drive Space Remaining

The Drive Space Remaining monitors are similar to the Drive Space Used monitors, but they tell you how much space remains instead of how much is in use.

The Drive Space Remaining monitors follow:

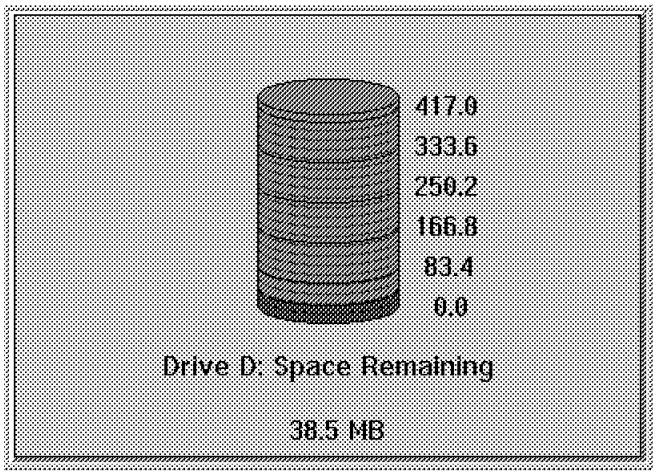


Figure 170. Drive Space Remaining Monitor - Real Time

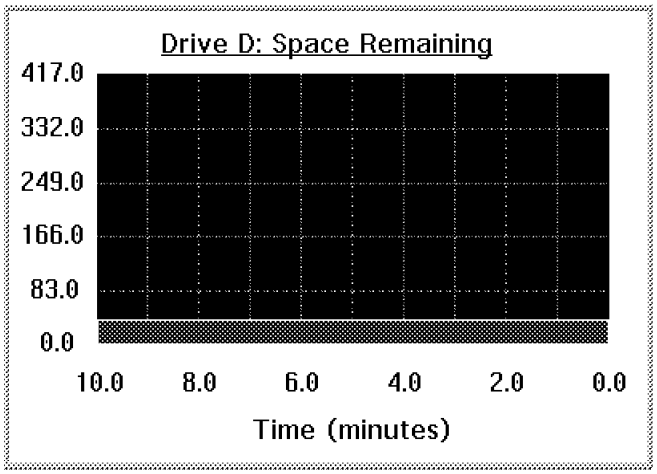


Figure 171. Drive Space Remaining Monitor - Line Graph

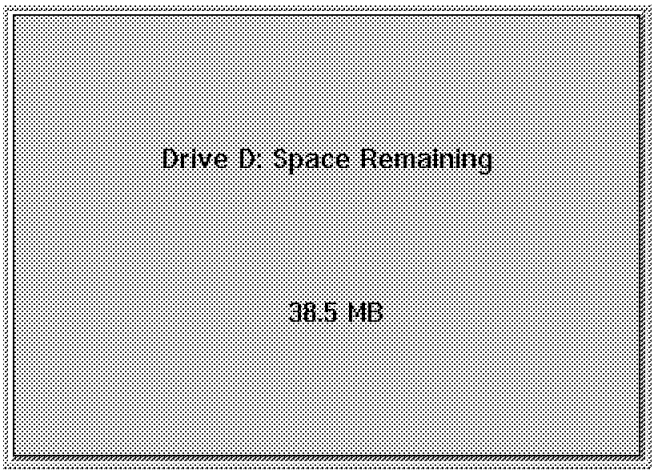


Figure 172. Drive Space Remaining Monitor - Text Display

Note: Every active hard disk drive has its own Drive Space Remaining monitor.

5.5.6 Print Jobs Queued

The Print Jobs Queued monitors follow:

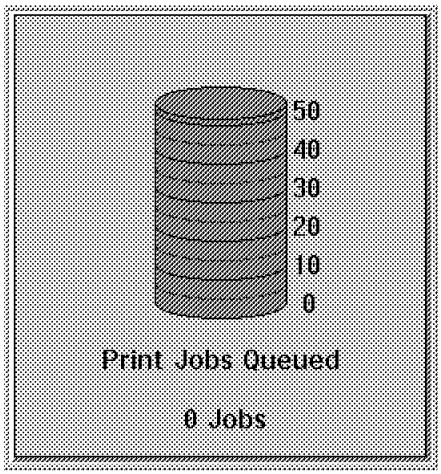


Figure 173. Print Jobs Queued Monitor - Real Time

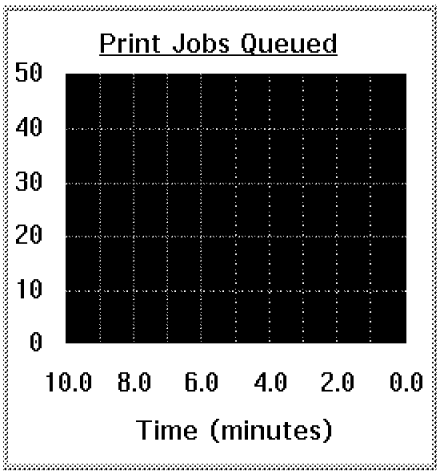


Figure 174. Print Jobs Queued - Line Graph

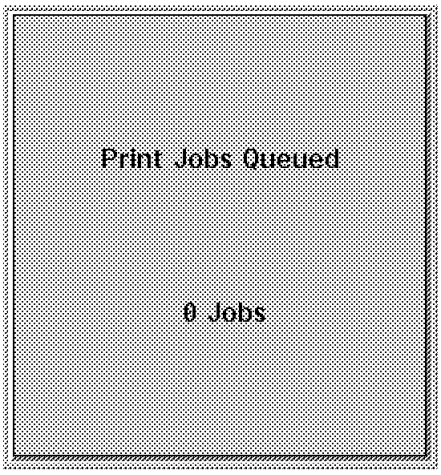


Figure 175. Print Jobs Queued - Text Display

This monitor makes sense especially if it is used at a print server.

5.5.7 Locked Memory

The Locked Memory monitors follow:

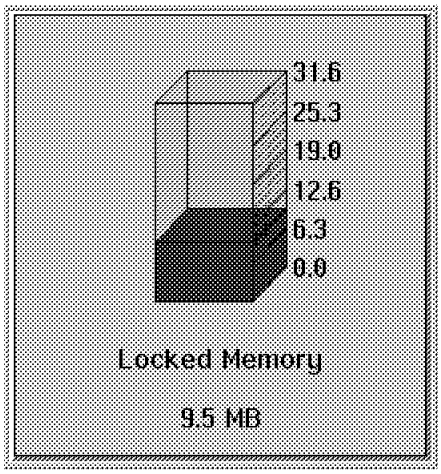


Figure 176. Locked Memory Monitor - Real Time

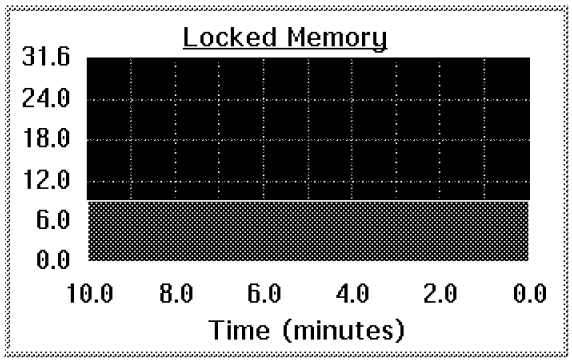


Figure 177. Locked Memory Monitor - Line Graph

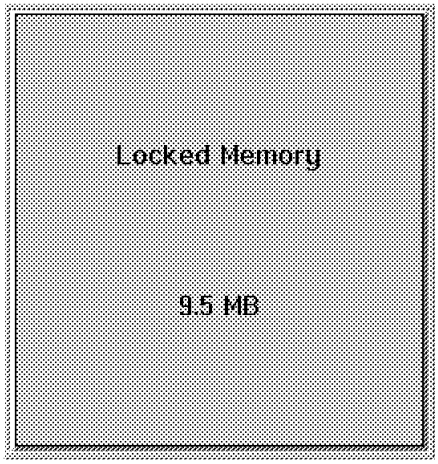


Figure 178. Locked Memory Monitor - Text Display

5.5.8 Memory Usage

The Memory Usage monitors follow:

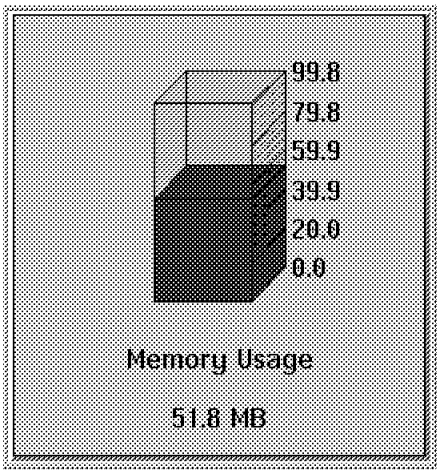


Figure 179. Memory Usage Monitor - Real Time

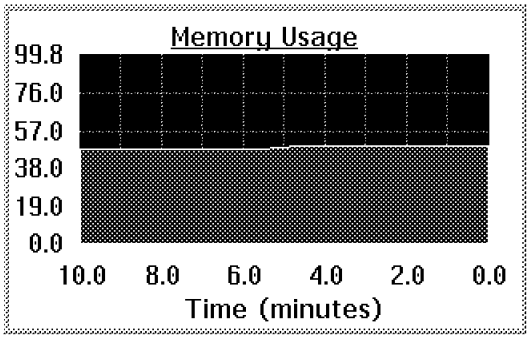


Figure 180. Memory Usage Monitor - Line Graph

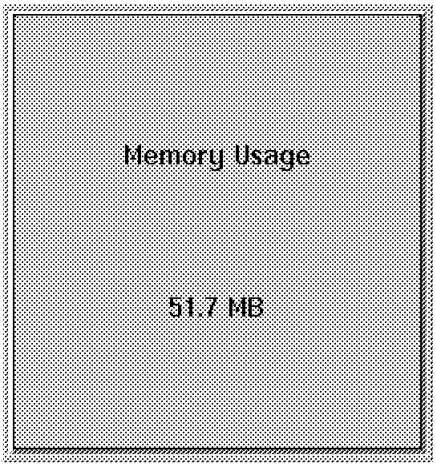


Figure 181. Memory Usage Monitor - Text Display

5.5.9 Swap File Size

The Swap File Size monitors follow:

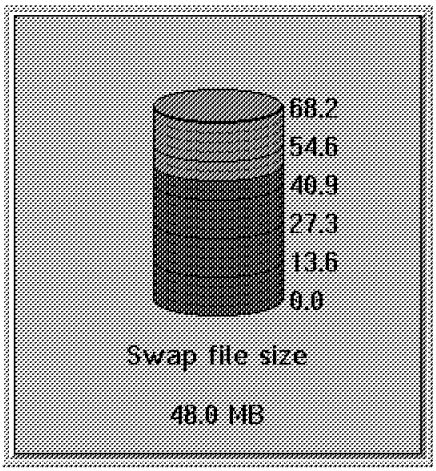


Figure 182. Swap File Size Monitor - Real Time

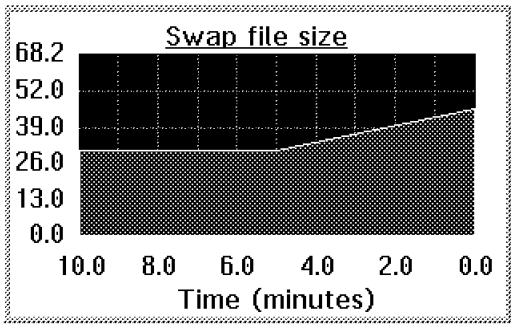


Figure 183. Swap File Size Monitor - Line Graph

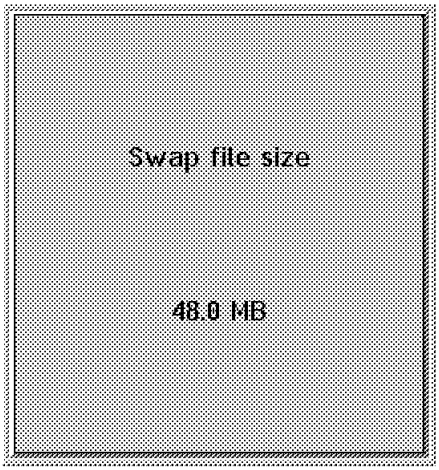


Figure 184. Swap File Size Monitor - Text Display

5.5.10 Swap Space Remaining

The Swap Space Remaining monitor looks as follows:

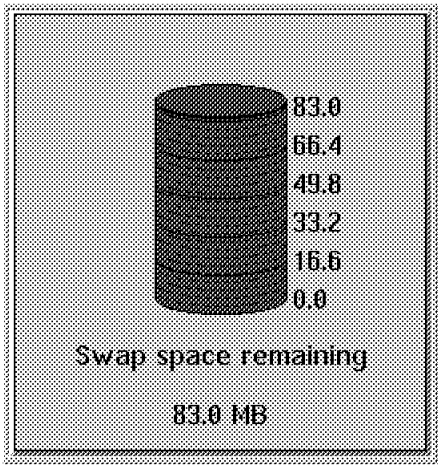


Figure 185. Swap Space Remaining Monitor - Real Time

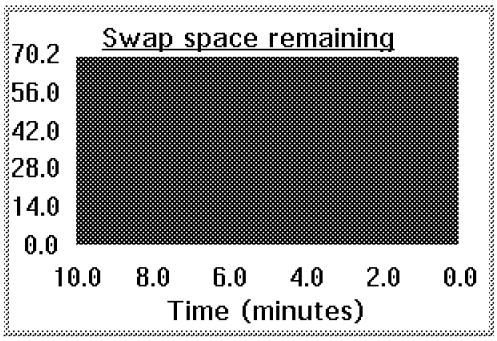


Figure 186. Swap Space Remaining - Line Graph

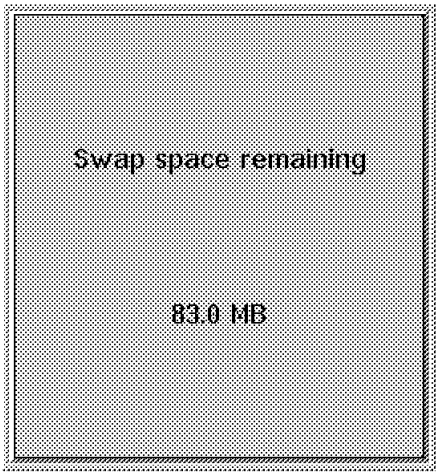


Figure 187. Swap Space Remaining Monitor - Text Display

5.5.11 Disk Workload

The Disk Workload monitors follow:

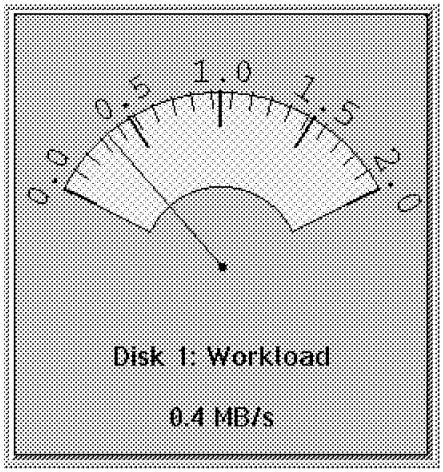


Figure 188. Disk Workload Monitor - Real Time

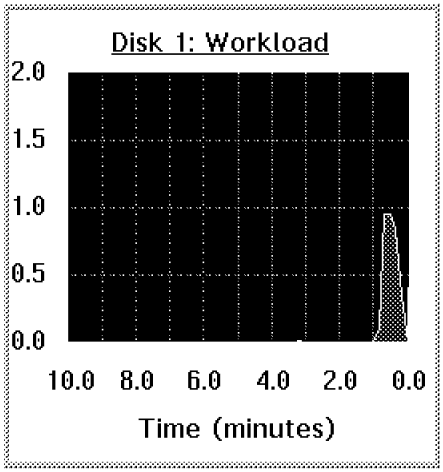


Figure 189. Disk Workload Monitor - Line Graph

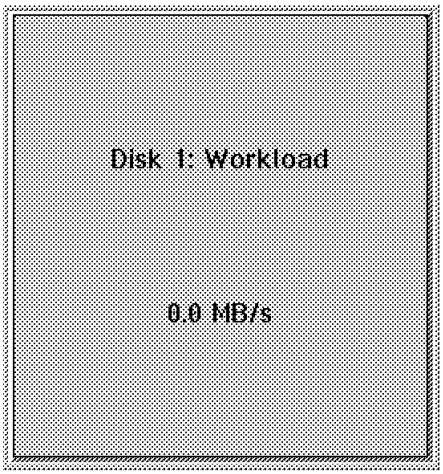


Figure 190. Disk Workload Monitor - Text Display

Note: There will be one Disk Workload monitor for every physical drive installed.

The Disk Workload monitor does *not* apply to raid devices.

5.5.12 Disk Error Rate

The Disk Error Rate monitors follow:

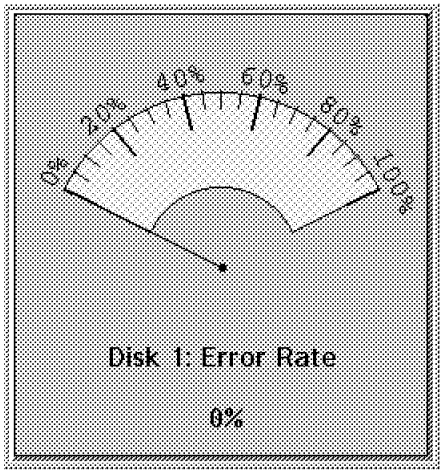


Figure 191. Disk Error Rate Monitor - Real Time

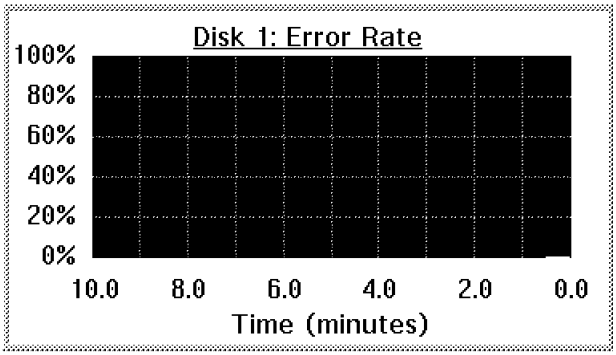


Figure 192. Disk Error Rate Monitor - Line Graph

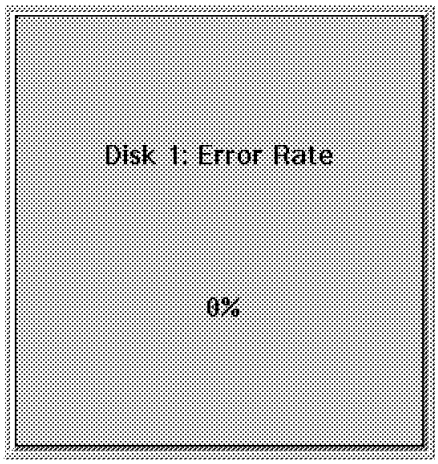


Figure 193. Disk Error Rate Monitor - Text Display

5.6 LAN Server Monitors

If you are running LAN Server on your workstation, you will have several additional monitors available to use in your automation activities or just to be alerted when specific conditions occur.

5.6.1 LAN Server: Sessions

The LAN Server: Session monitors follow:

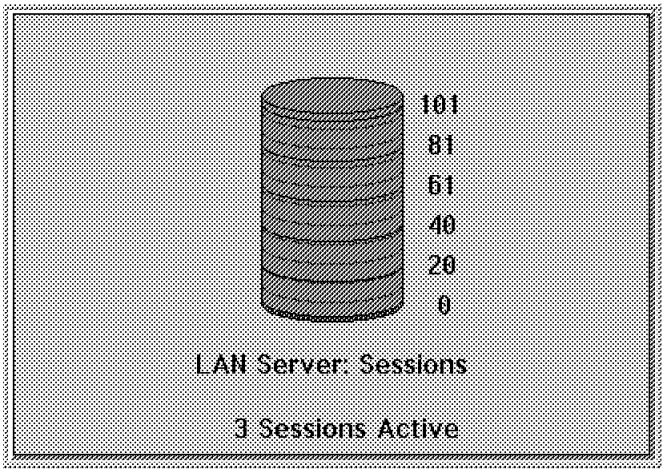


Figure 194. LAN Server: Sessions Monitor - Real Time Layout

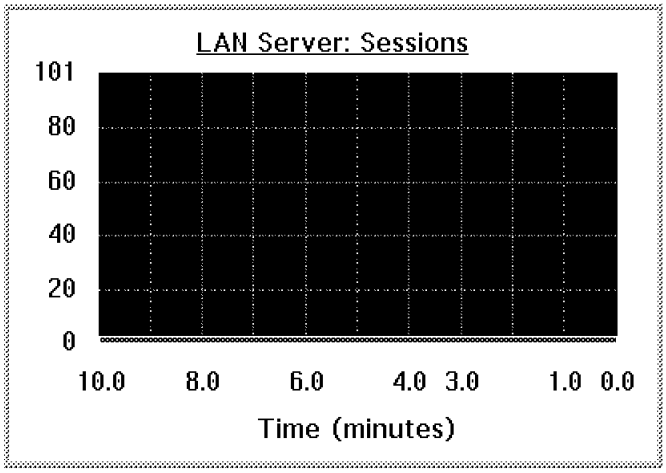


Figure 195. LAN Server: Sessions Monitor - Line Graph Layout

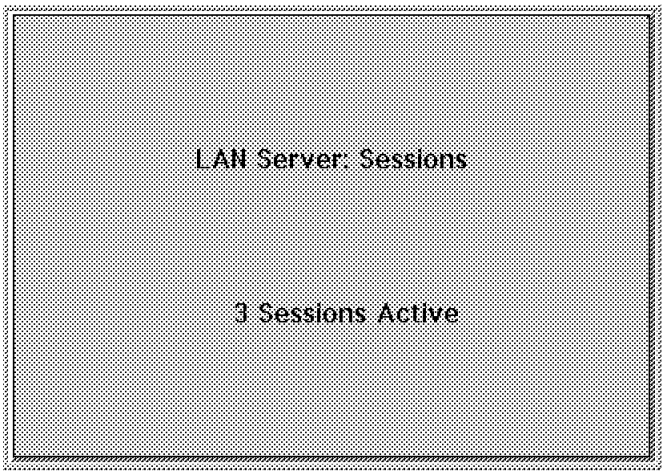


Figure 196. LAN Server: Sessions Monitor - Text Display Layout

5.6.2 LAN Server: Connections

The LAN Server: Connections monitors follow:

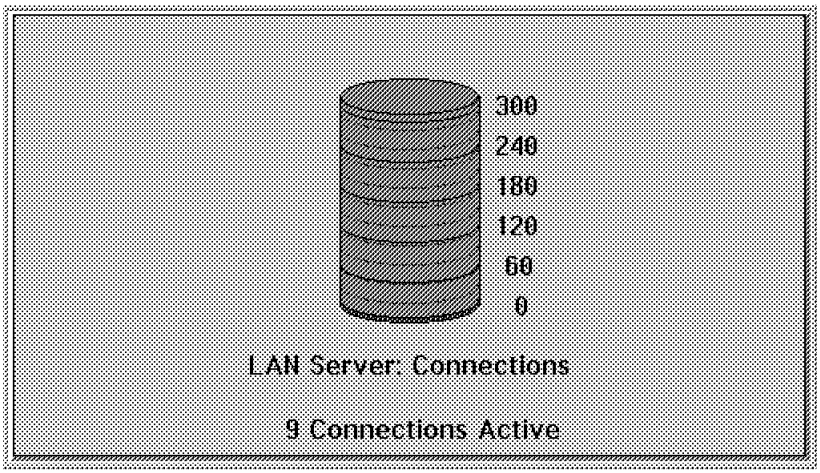


Figure 197. LAN Server: Connections Monitor - Real Time Layout

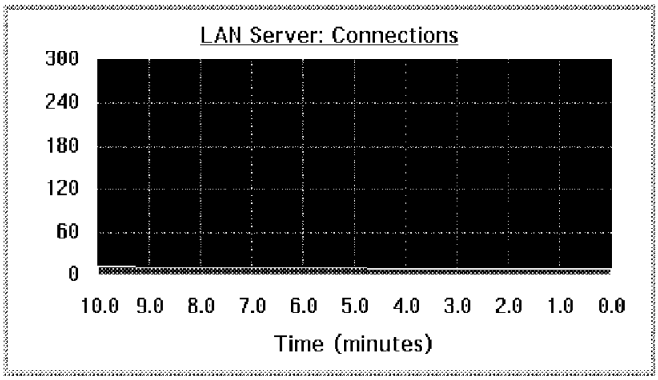


Figure 198. LAN Server: Connections Monitor - Line Graph Layout

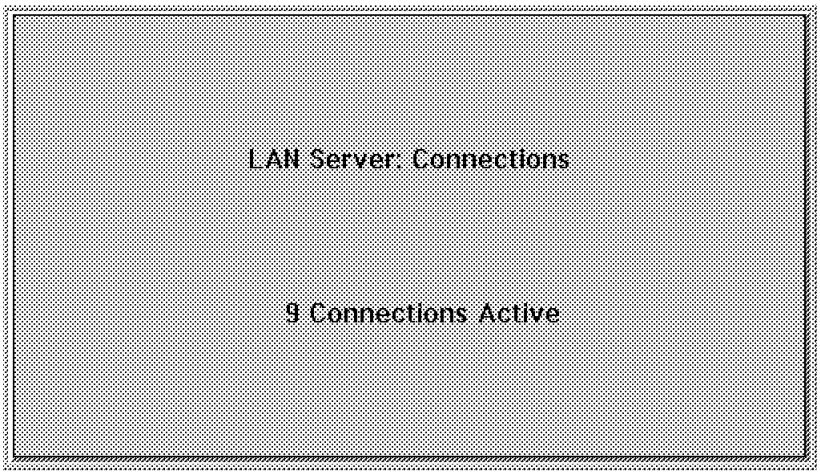


Figure 199. LAN Server: Connections Monitor - Text Display Layout

5.6.3 LAN Server: Opens

The LAN Server: Open monitors follows:

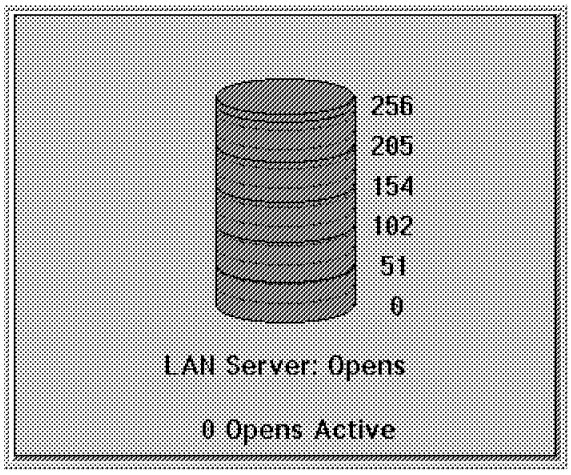


Figure 200. LAN Server: Opens Monitor - Real Time Layout

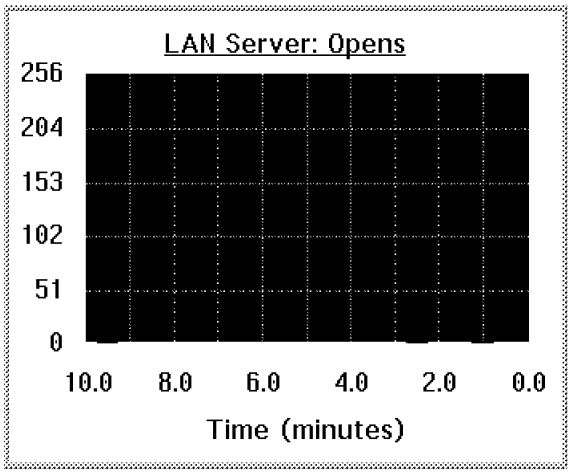


Figure 201. LAN Server: Opens Monitor - Line Graph Layout

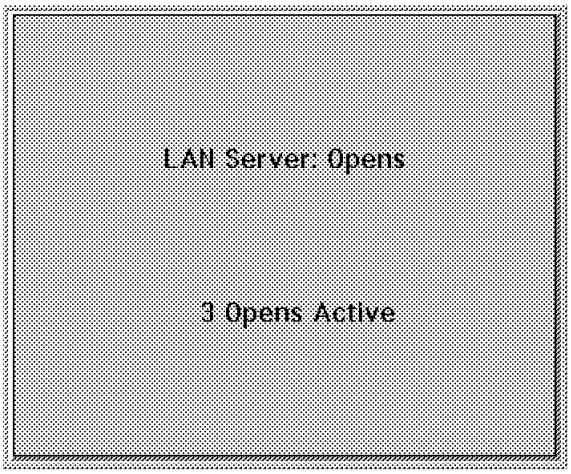


Figure 202. LAN Server: Opens Monitor - Text Display Layout

5.6.4 LAN Server: Shares

The LAN Server: Shares monitors follow:

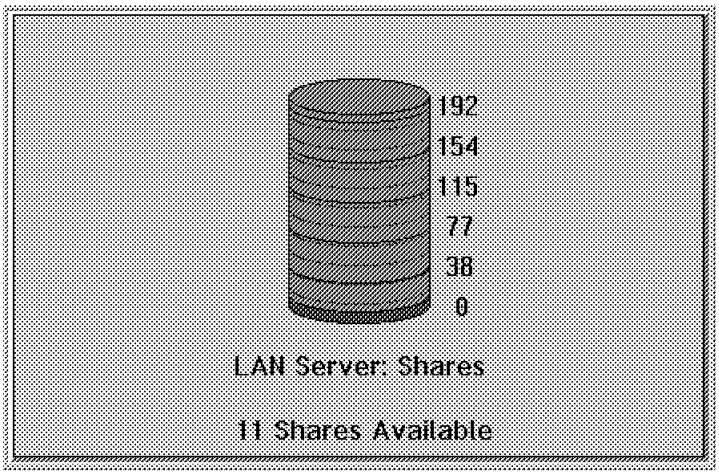


Figure 203. LAN Server: Shares Monitor - Real Time Layout

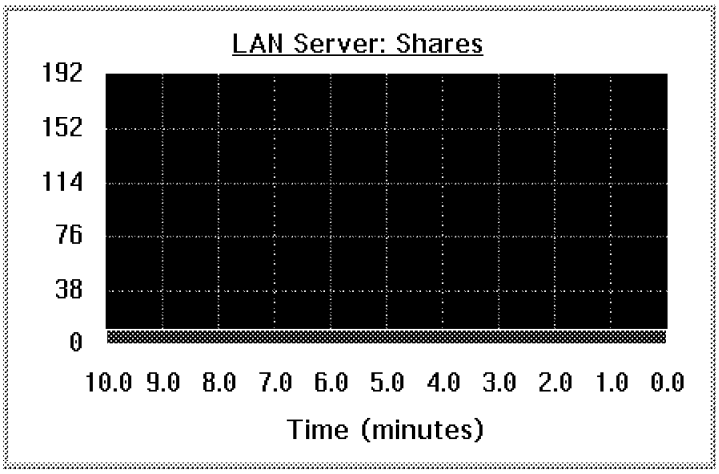


Figure 204. LAN Server: Shares Monitor - Line Graph Layout

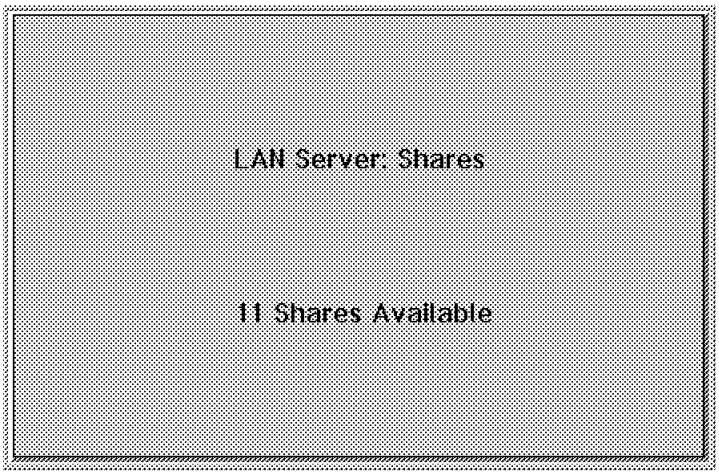


Figure 205. LAN Server: Shares Monitor - Text Display Layout

5.6.5 LAN Server: Bytes Sent

The LAN Server: Bytes Sent monitors follow:

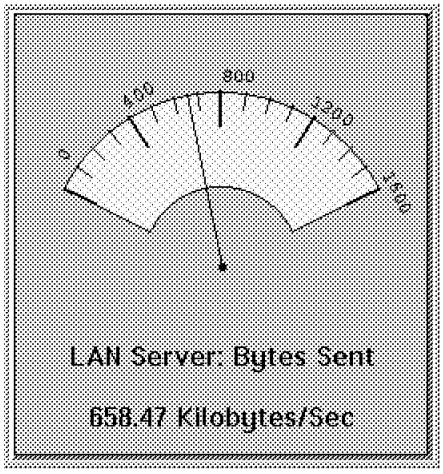


Figure 206. LAN Server: Bytes Sent Monitor - Real Time Layout

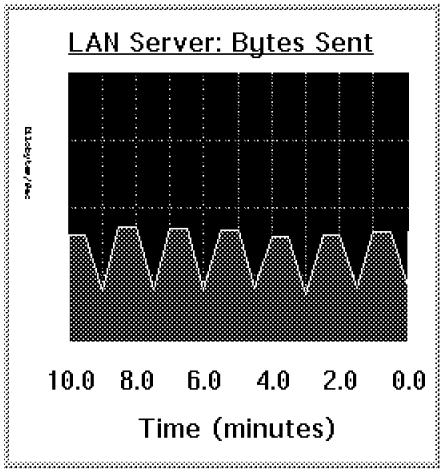


Figure 207. LAN Server: Bytest Sent - Line Graph Layout

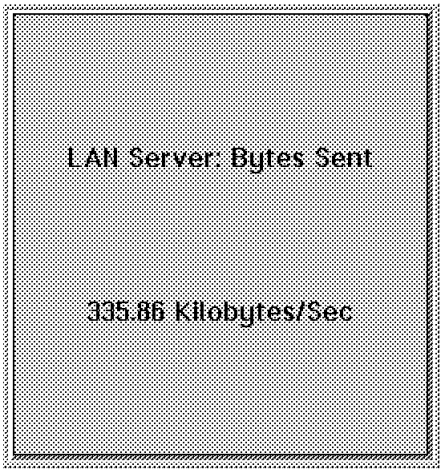


Figure 208. LAN Server: Bytes Sent Monitor - Text Display Layout

5.6.6 LAN Server: Bytes Received

The LAN Server: Bytes Received monitors follow:

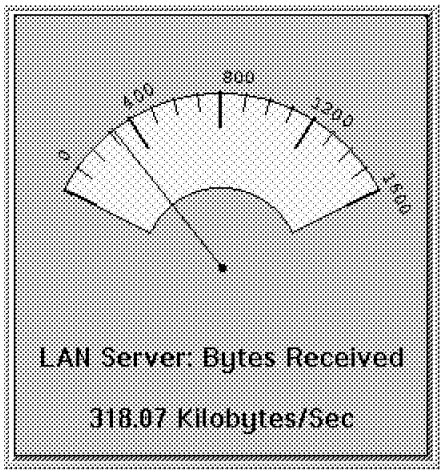


Figure 209. LAN Server: Bytes Received Monitor - Real Time Layout

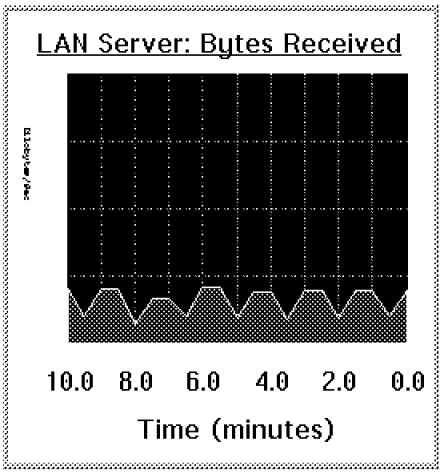


Figure 210. LAN Server: Bytest Received - Line Graph Layout

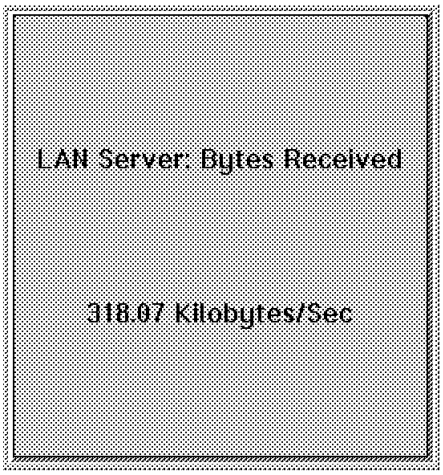


Figure 211. LAN Server: Bytes Received Monitor - Text Display Layout

5.6.7 LAN Server: Response Time

The LAN Server: Response Time monitors follow:

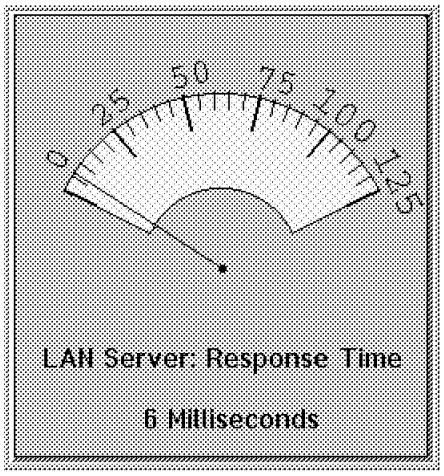


Figure 212. LAN Server: Response Time Monitor - Real Time Layout

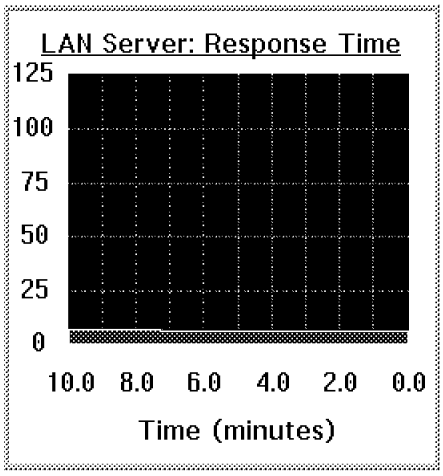


Figure 213. LAN Server: Response Time - Line Graph Layout

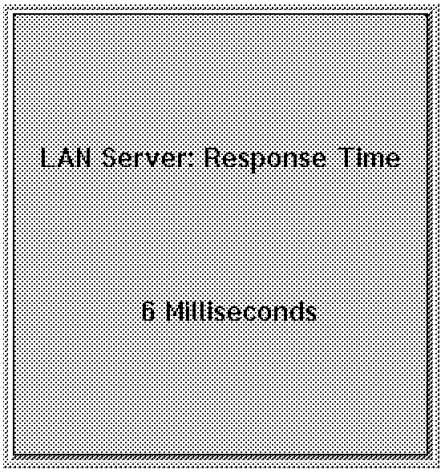


Figure 214. LAN Server: Response Time Monitor - Text Display Layout

5.6.8 LAN Server: Buffer Shortage

The LAN Server: Buffer Shortage monitors follow:

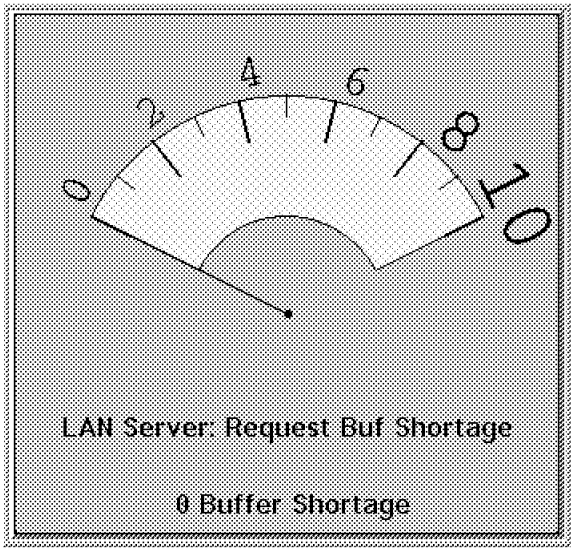


Figure 215. LAN Server: Buffer Shortage Monitor - Real Time Layout

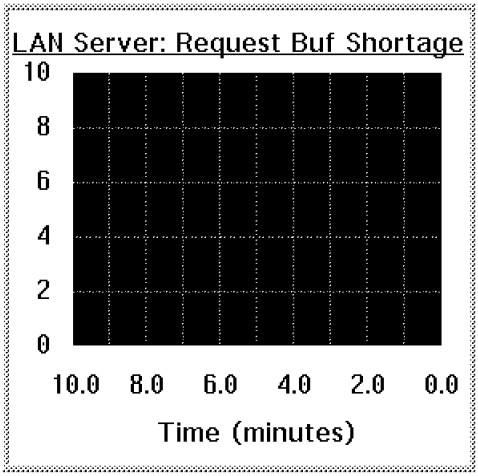


Figure 216. LAN Server: Buffer Shortage Monitor - Line Graph Layout

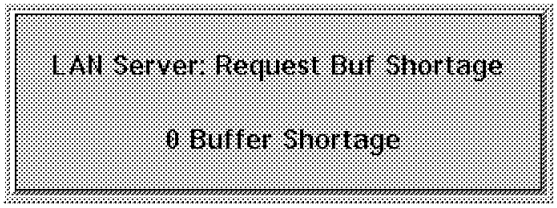


Figure 217. LAN Server: Buffer Shortage Monitor - Text Display Layout

5.7 TCP/IP-Related Monitors

The following screen captures are all related to TCP/IP monitors.

5.7.1 UDP Datagrams Sent

The UDP Datagrams Sent monitors follow:

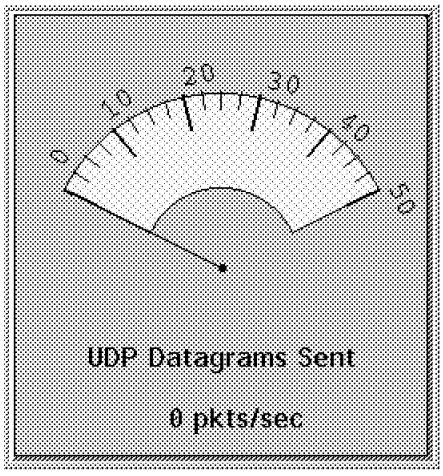


Figure 218. UDP Datagrams Sent Monitor - Real Time Layout

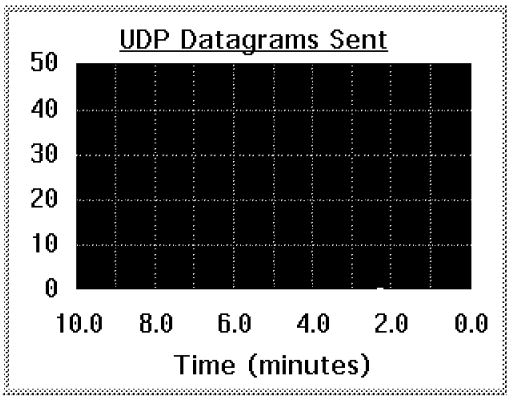


Figure 219. UDP Datagrams Sent Monitor - Line Graph Layout

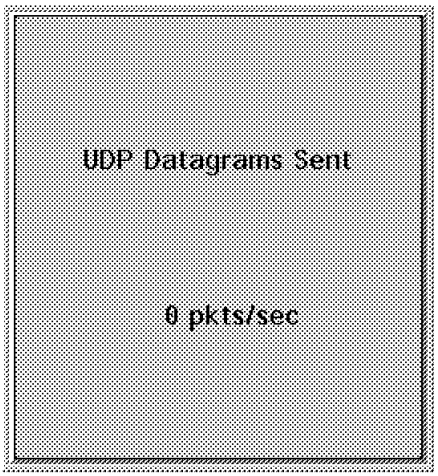


Figure 220. UDP Datagrams Sent Monitor - Text Display Layout

5.7.2 UDP Datagrams Received

The UDP Datagrams Received monitors follow:

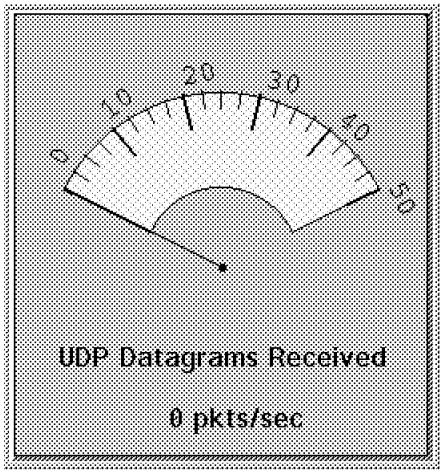


Figure 221. UDP Datagrams Received Monitor - Real Time Layout

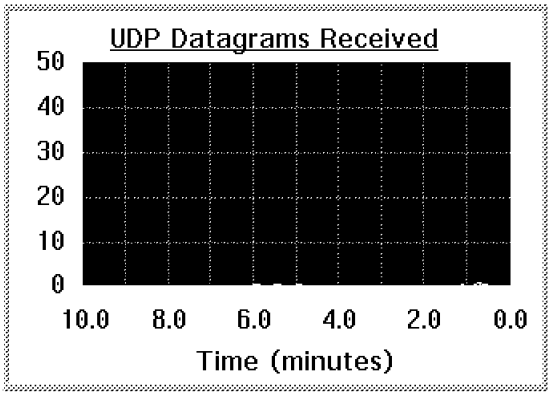


Figure 222. UDP Datagrams Received Monitor - Line Graph Layout

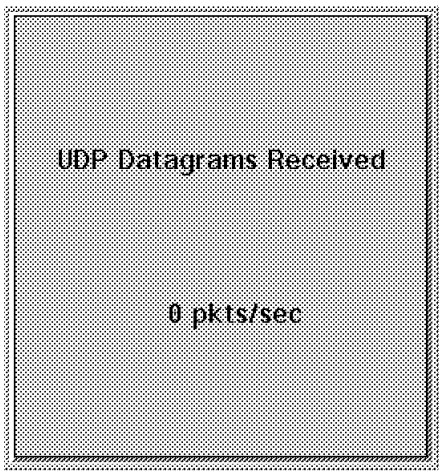


Figure 223. UDP Datagrams Received Monitor - Text Display Layout

5.7.3 IP Packets Sent

The IP Packets Sent monitors follow:

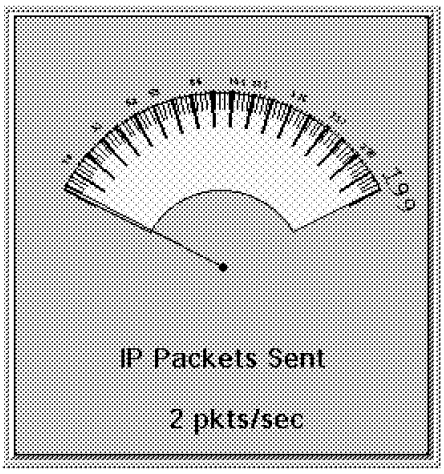


Figure 224. IP Packets Sent Monitor - Real Time Layout

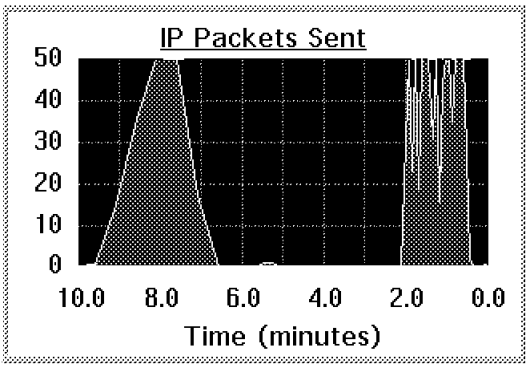


Figure 225. IP Packets Sent Monitor - Line Graph Layout

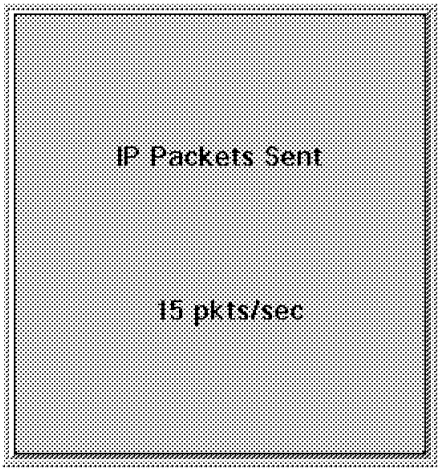


Figure 226. IP Packets Sent Monitor - Text Display Layout

5.7.4 IP Packets Received

The IP Packets Received monitors follow:

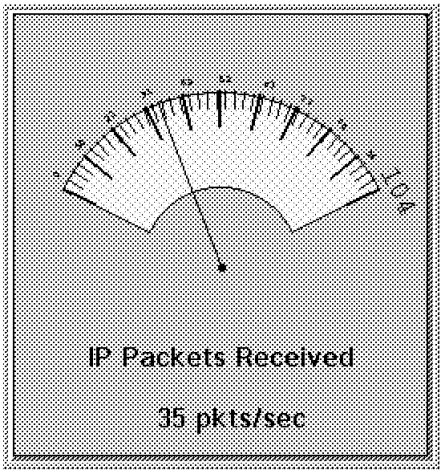


Figure 227. IP Packets Received Monitor - Real Time Layout

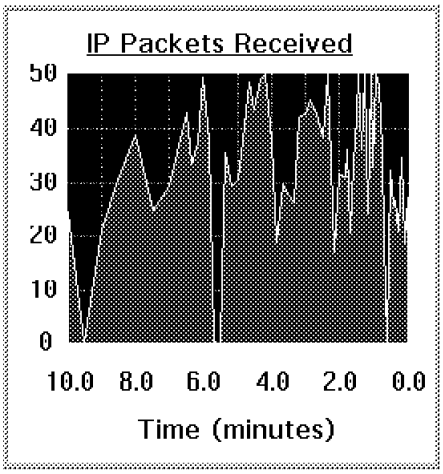


Figure 228. IP Packets Received Monitor - Line Graph Layout

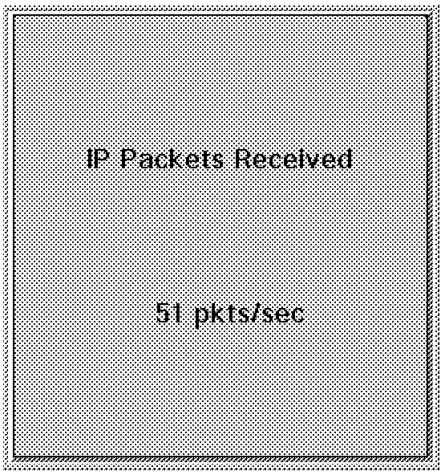


Figure 229. IP Packets Received Monitor - Text Display Layout

5.7.5 IP Packets Received with Errors

The IP Packets Received with Errors monitors follow:

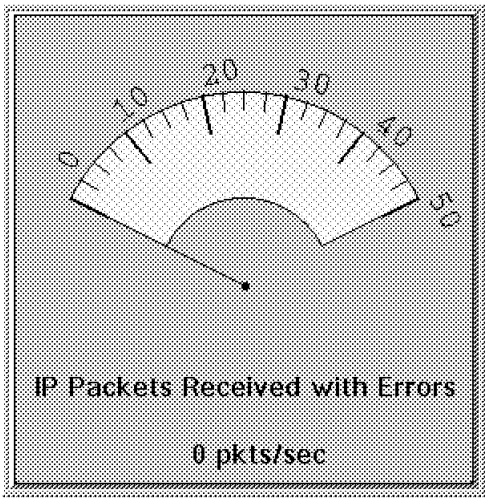


Figure 230. IP Packets Received with Errors Monitor - Real Time Layout

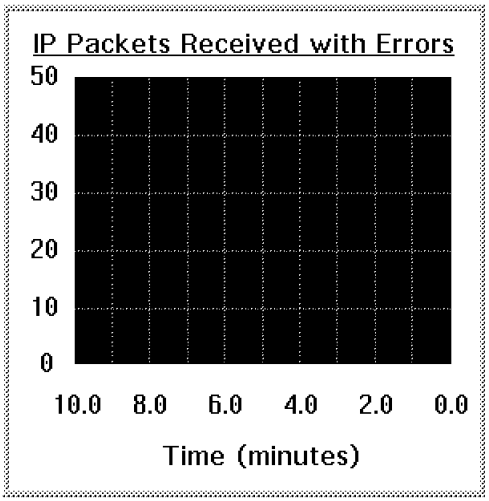


Figure 231. IP Packets Received with Errors Monitor - Line Graph Layout

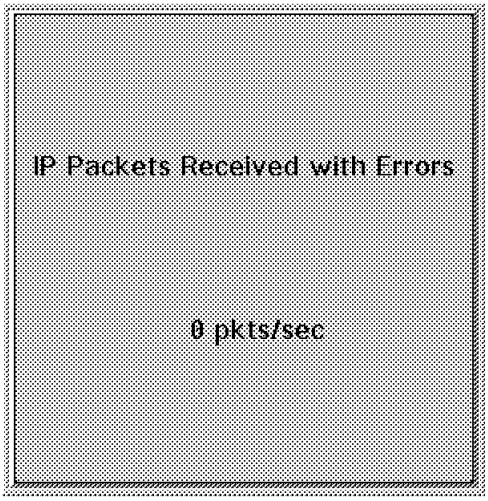


Figure 232. IP Packets Received with Errors Monitor - Text Display Layout

5.7.6 TCP Connections

The TCP Connections monitors follow:

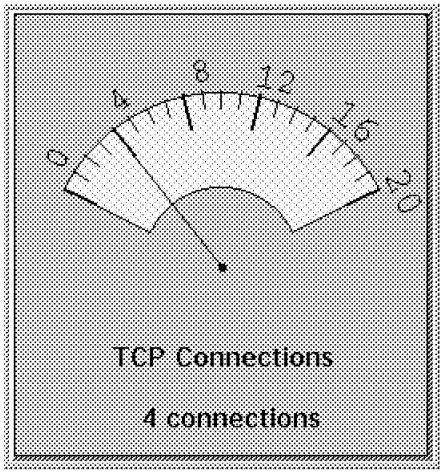


Figure 233. TCP Connections Monitor - Real Time Layout

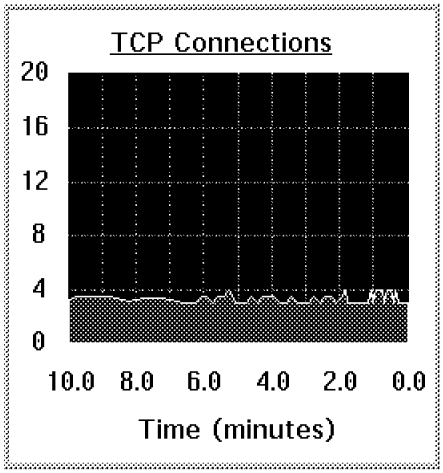


Figure 234. TCP Connections Monitor - Line Graph Layout

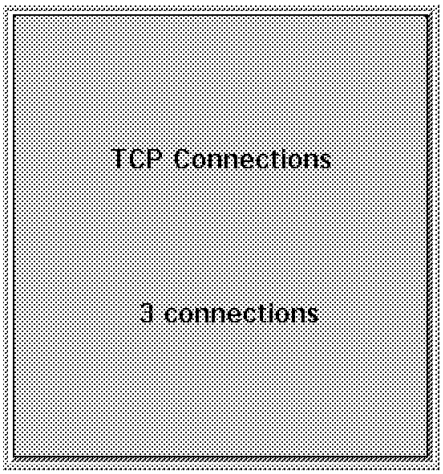


Figure 235. TCP Connections Monitor - Text Display Layout

5.7.7 TCP/IP Sockets

The TCP/IP Sockets monitors follow:

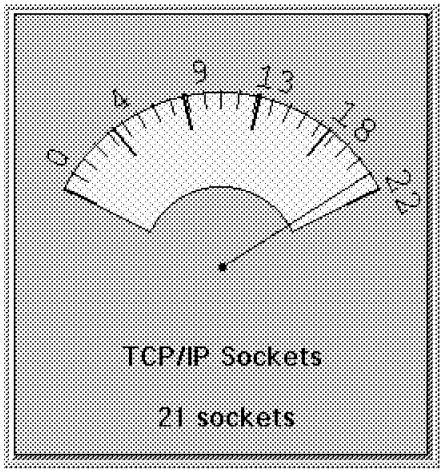


Figure 236. TCP/IP Sockets Monitor - Real Time Layout

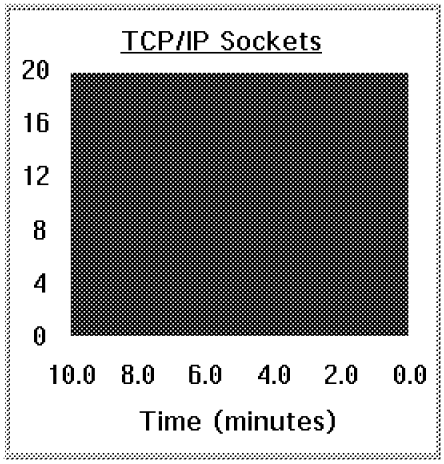


Figure 237. TCP/IP Sockets Monitor - Line Graph Layout

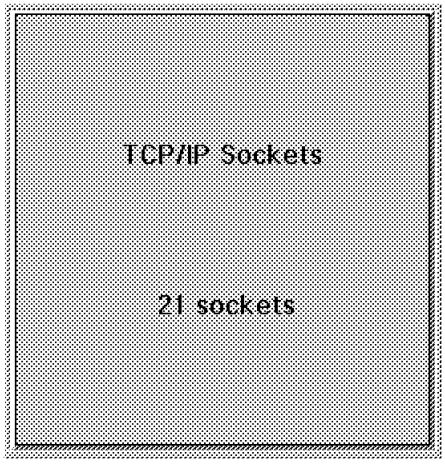


Figure 238. TCP/IP Sockets Monitor - Text Display Layout

5.7.8 TCP/IP Interface - Unicast Packets Sent

The TCP/IP Interface - Unicast Packets Sent monitors follow:

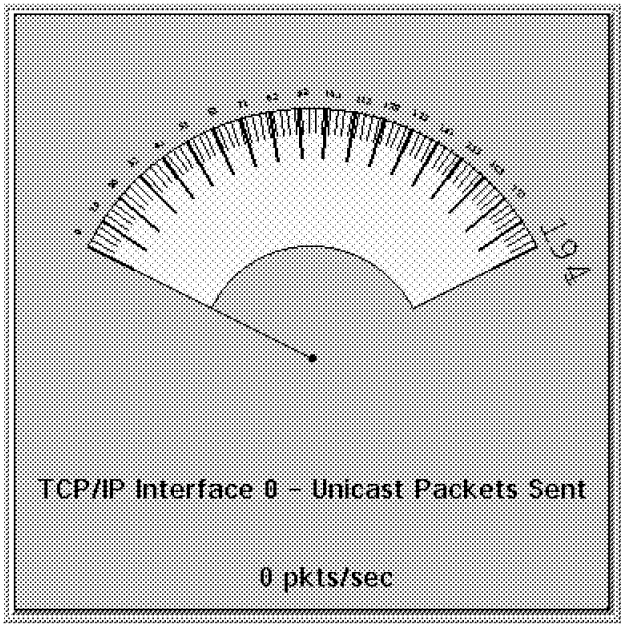


Figure 239. TCP/IP Interface - Unicast Packets Sent Monitor - Real Time Layout

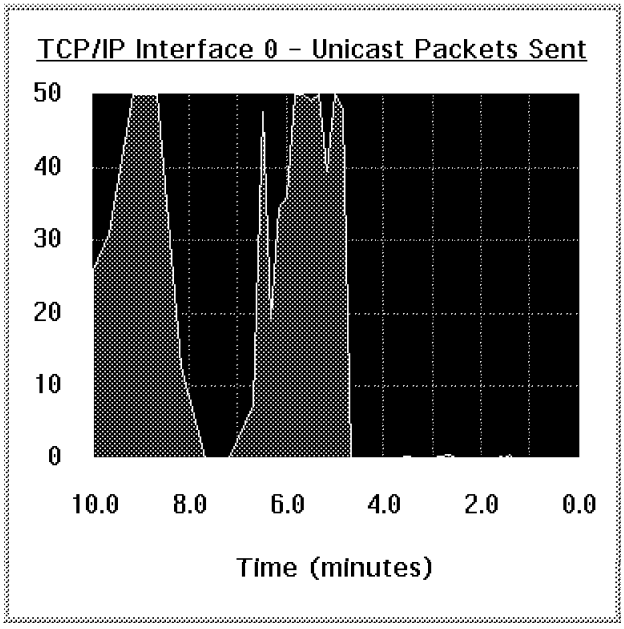


Figure 240. TCP/IP Interface - Unicast Packets Sent Monitor - Line Graph Layout

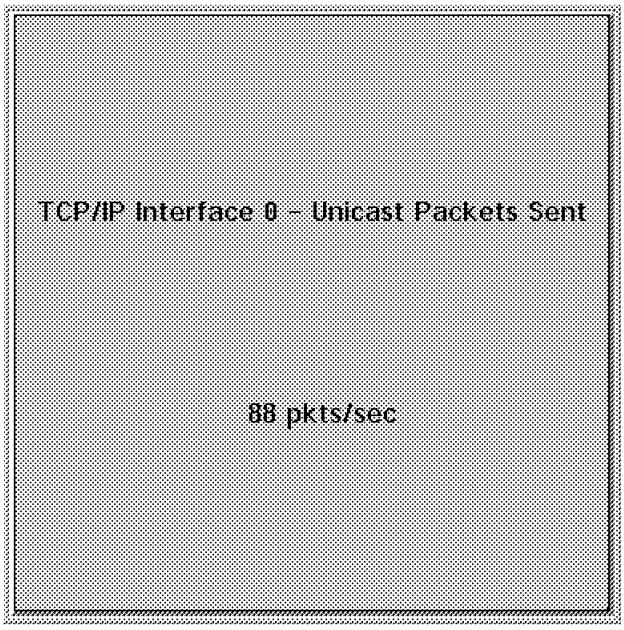


Figure 241. TCP/IP Interface - Unicast Packets Sent Monitor - Text Display Layout

Note: One Unicast Packets Sent monitor is delivered for each TCP/IP interface installed on the machine. The installed interfaces are numbered ascending sequentially starting with *0*.

5.7.9 TCP/IP Interface - Broadcast Packets Sent

The TCP/IP Interface - Broadcast Packets Sent monitors follow:

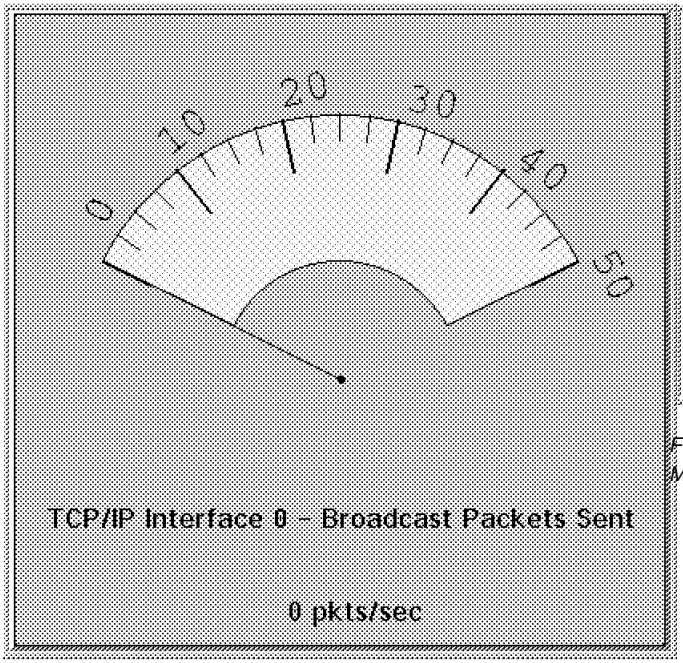


Figure 242. TCP/IP Interface - Broadcast Packets Sent Monitor - Real Time Layout

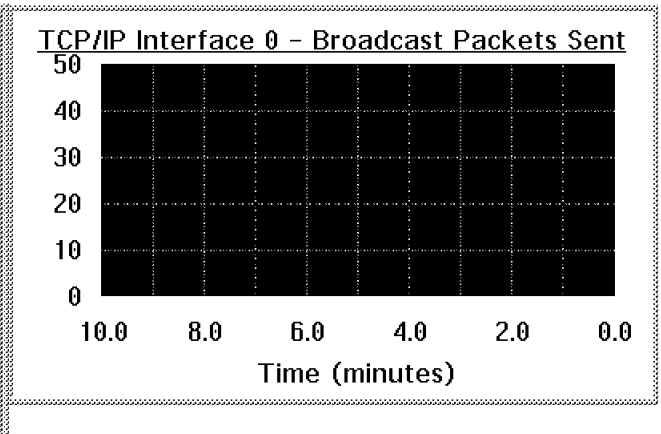


Figure 243. TCP/IP Interface - Broadcast Packets Sent Monitor - Line Graph Layout

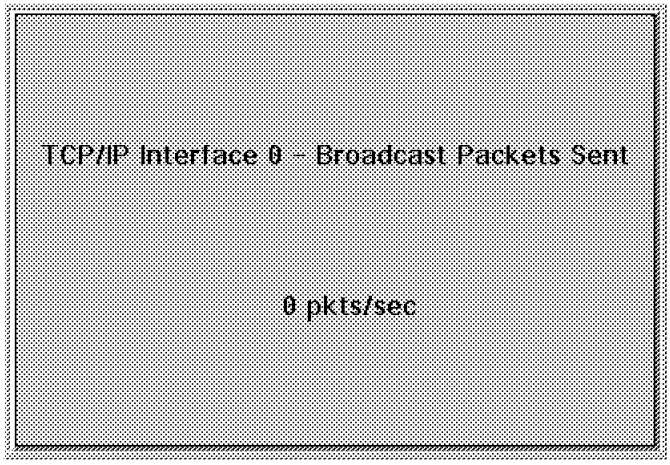


Figure 244. TCP/IP Interface - Broadcast Packets Sent Monitor - Text Display Layout

Note: One Broadcast Packets Sent monitor is delivered for each TCP/IP interface installed on the machine. The installed interfaces are numbered ascending sequentially starting with *0*.

5.7.10 TCP/IP Interface - Bytes Sent

The TCP/IP Interface - Bytes Sent monitors follow:

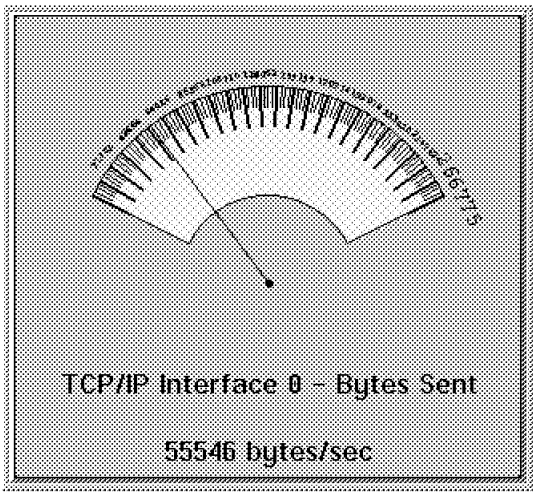


Figure 245. TCP/IP Interface - Bytes Sent Monitor - Real Time Layout

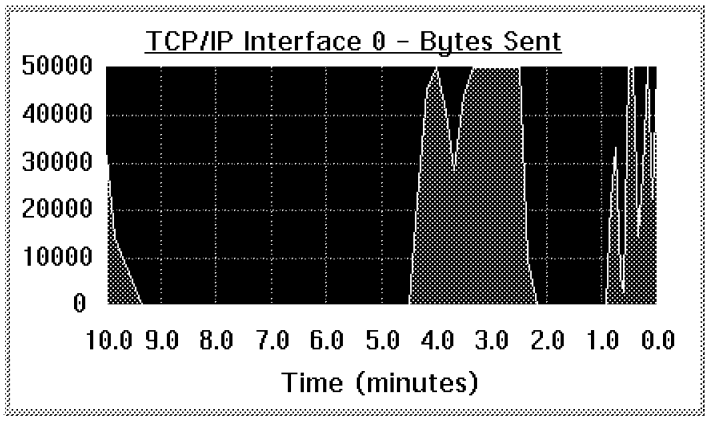


Figure 246. TCP/IP Interface - Bytes Sent Monitor - Line Graph Layout

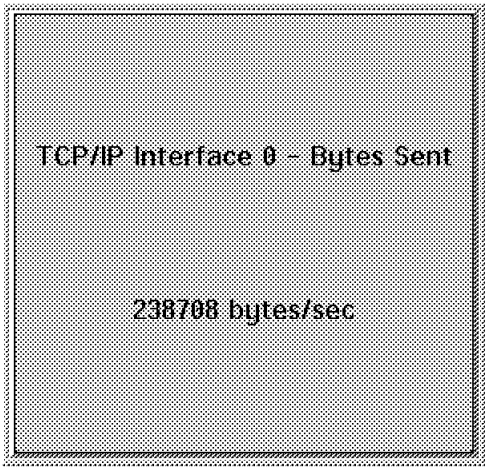


Figure 247. TCP/IP Interface - Bytes Sent Monitor - Text Display Layout

Note: One Bytes Sent monitor is delivered for each TCP/IP interface installed on the machine. The installed interfaces are numbered ascending sequentially starting from *0*.

5.7.11 TCP/IP Interface - Unicast Packets Received

The TCP/IP Interface - Unicast Packets Received monitors follow:

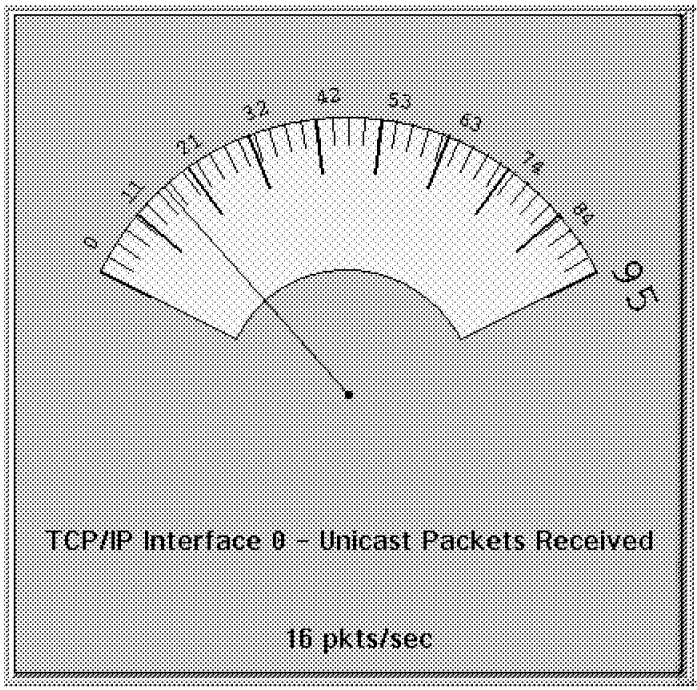


Figure 248. TCP/IP Interface - Unicast Packets Received Monitor - Real Time Layout

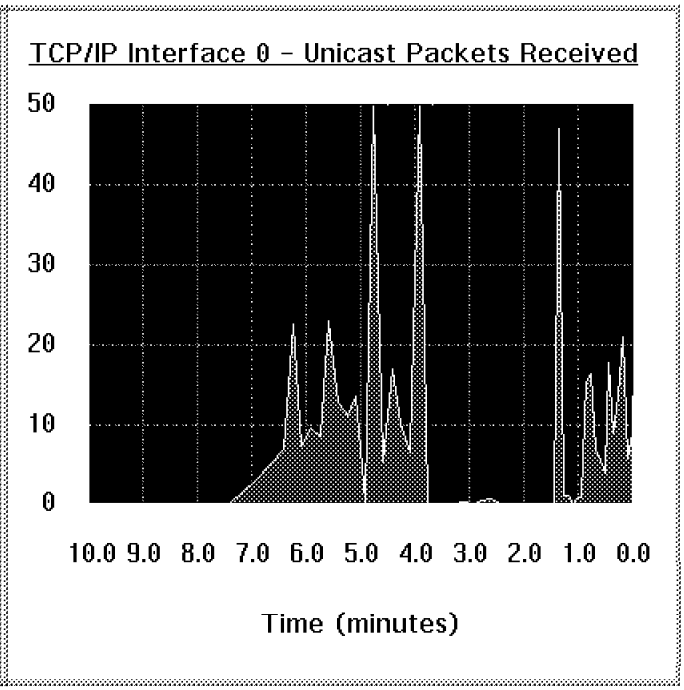


Figure 249. TCP/IP Interface - Unicast Packets Received Monitor - Line Graph Layout

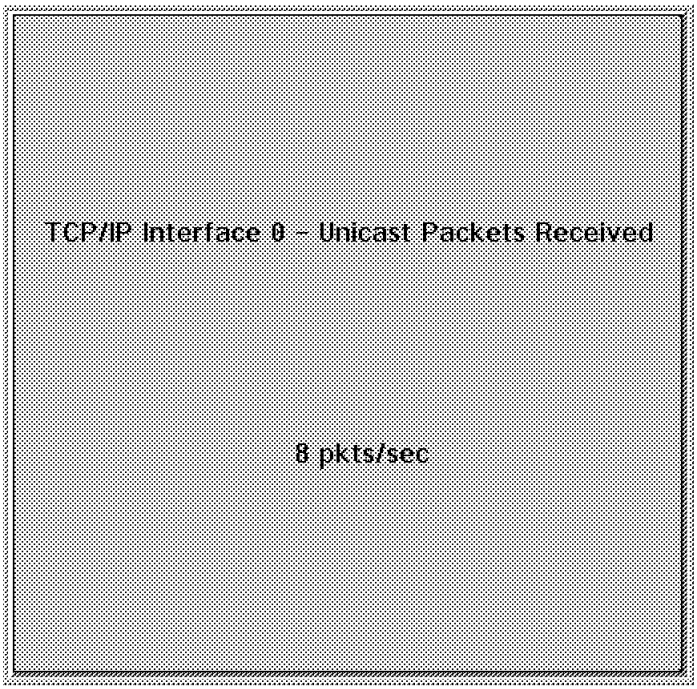


Figure 250. TCP/IP Interface - Unicast Packets Received Monitor - Text Display Layout

Note: One Unicast Packets Received monitor is delivered for each TCP/IP interface installed on the machine. The installed interfaces are numbered ascending sequentially starting from *0*.

5.7.12 TCP/IP Interface - Broadcast Packets Received

The TCP/IP Interface - Broadcast Packets Received monitors follow:

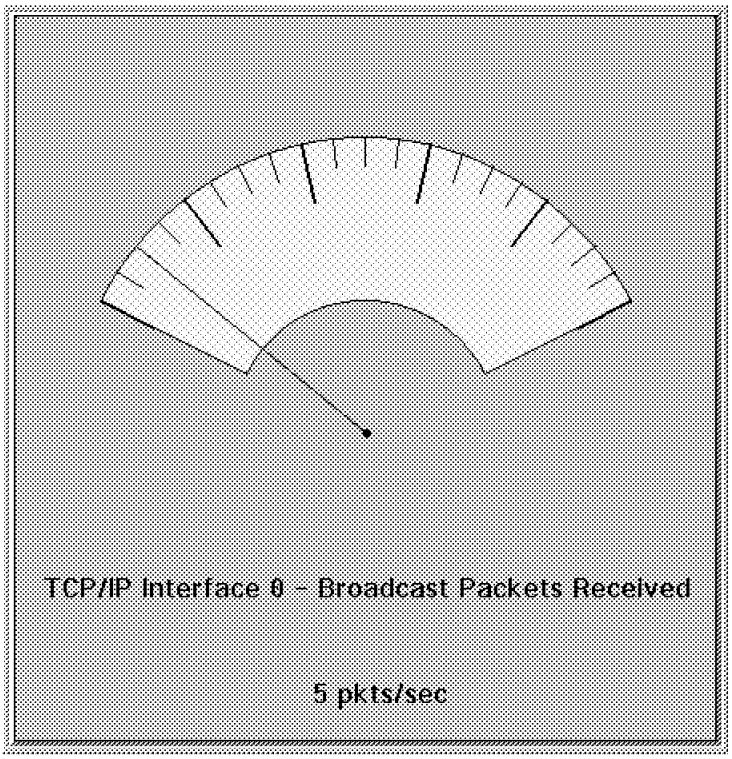


Figure 251. TCP/IP Interface - Broadcast Packets Received Monitor - Real Time Layout

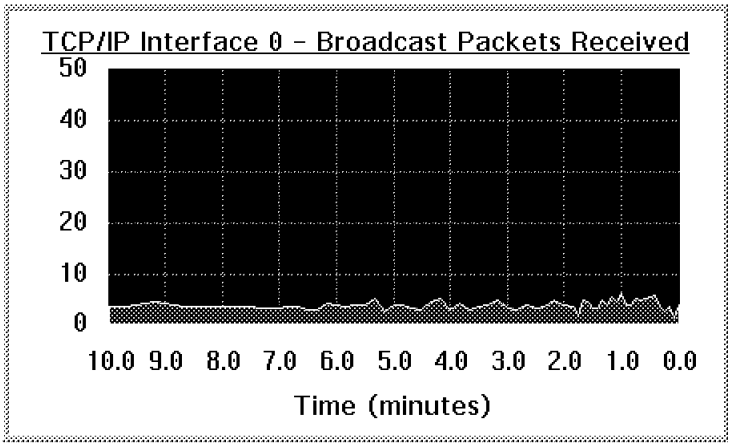


Figure 252. TCP/IP Interface - Broadcast Packets Received Monitor - Line Graph Layout

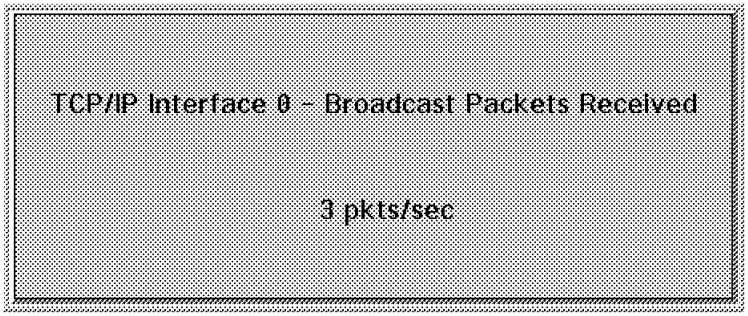


Figure 253. TCP/IP Interface - Broadcast Packets Received Monitor - Text Display Layout

Note: One Broadcast Packets Received monitor is delivered for each TCP/IP interface installed on the machine. The installed interfaces are numbered ascending sequentially starting from *0*.

5.7.13 TCP/IP Interface - Bytes Received

The TCP/IP Interface - Bytes Received monitors follow:

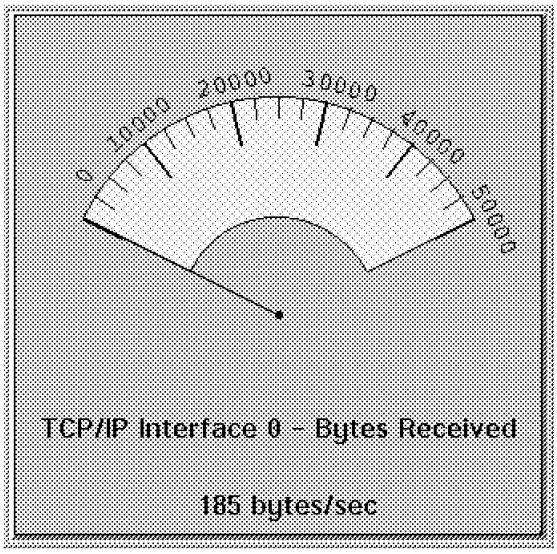


Figure 254. TCP/IP Interface - Bytes Received Monitor - Real Time Layout

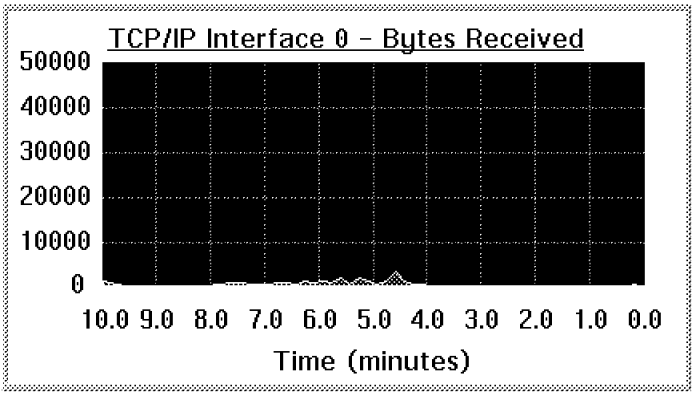


Figure 255. TCP/IP Interface - Bytes Received Monitor - Line Graph Layout

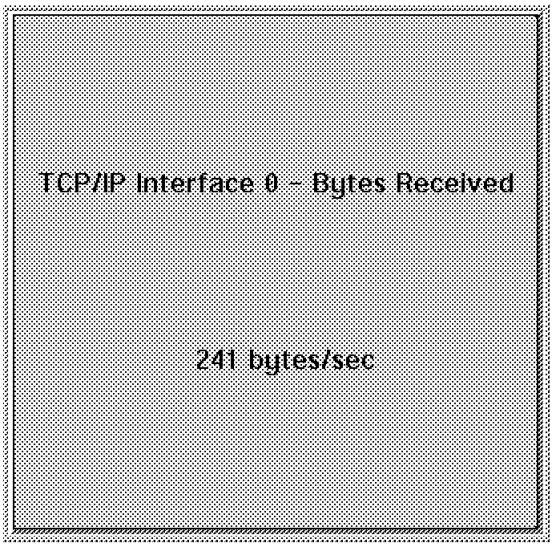


Figure 256. TCP/IP Interface - Bytes Received Monitor - Text Display Layout

Note: One Bytes Received monitor is delivered for each TCP/IP interface installed on the machine. The installed interfaces are numbered ascending sequentially from *0*.

5.8 Monitors Related to special Hardware

The following monitors will only appear on your system if you have the hardware associated with them.

5.8.1 Thinkpad: Battery Remaining

The Battery Remaining monitors follow:

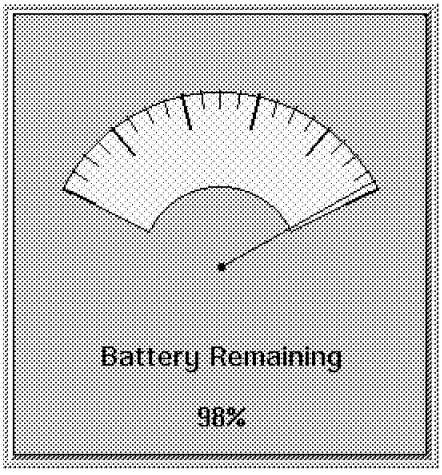


Figure 257. Battery Remaining Monitor - Real Time

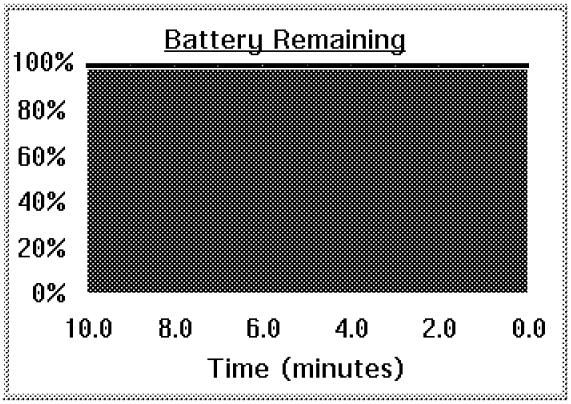


Figure 258. Battery Remaining Monitor - Line Graph

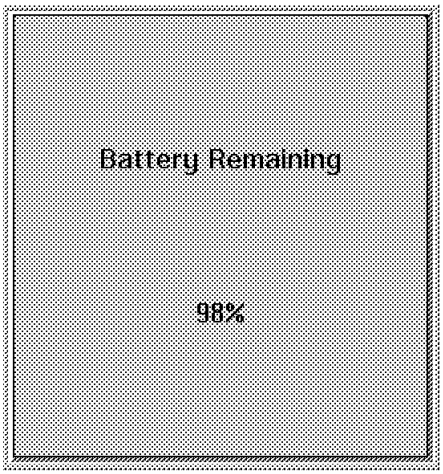


Figure 259. Battery Remaining Monitor - Text Display

5.8.2 ServerGuard Adapter: System Temperature

The System Temperature monitors follow:

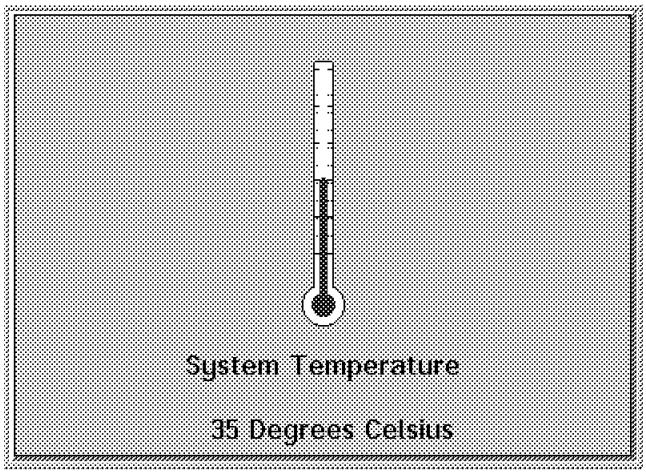


Figure 260. System Temperature Monitor - Real Time

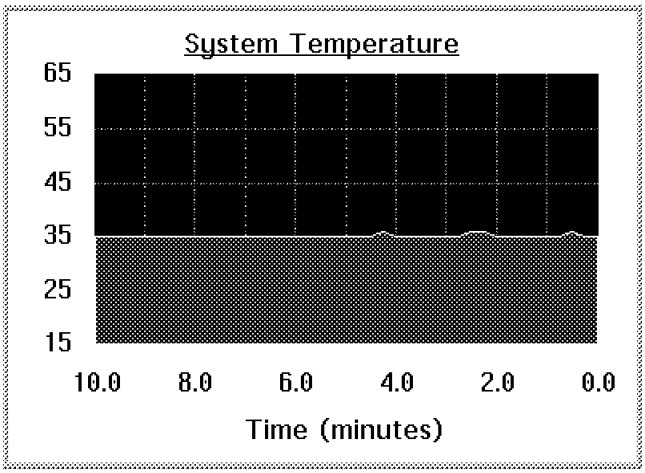


Figure 261. System Temperature Monitor - Line Graph

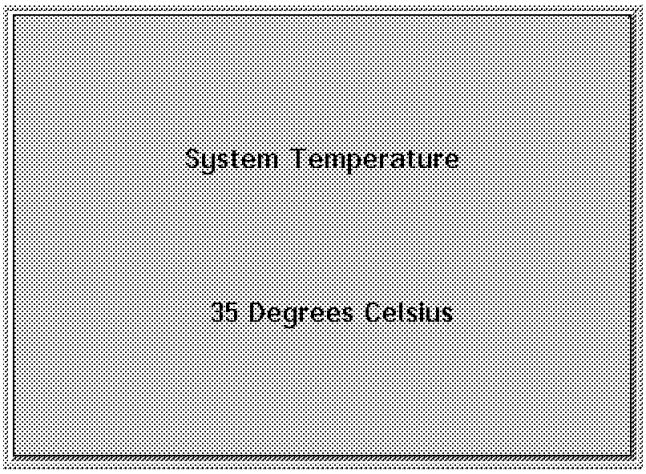


Figure 262. System Temperature Monitor - Text Display

5.8.3 ServerGuard Adapter: 5Volt Power Supply Voltage

The 5Volt power supply voltage monitors follow:

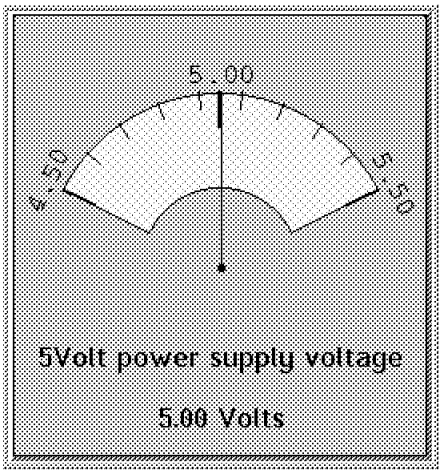


Figure 263. 5Volt Power Supply Voltage Monitor - Real Time

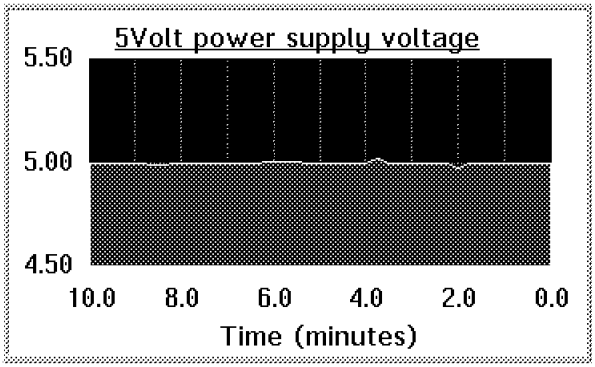


Figure 264. 5Volt Power Supply Voltage Monitor - Line Graph

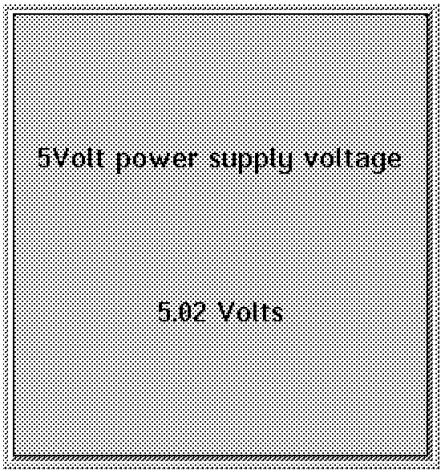


Figure 265. 5Volt Power Supply Voltage Monitor - Text Display

5.8.4 ServerGuard Adapter: 12Volt Power Supply Voltage

The 12Volt power supply voltage monitors follow:

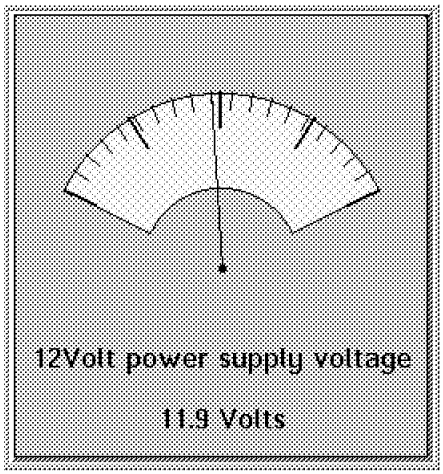


Figure 266. 12Volt Power Supply Voltage Monitor - Real Time

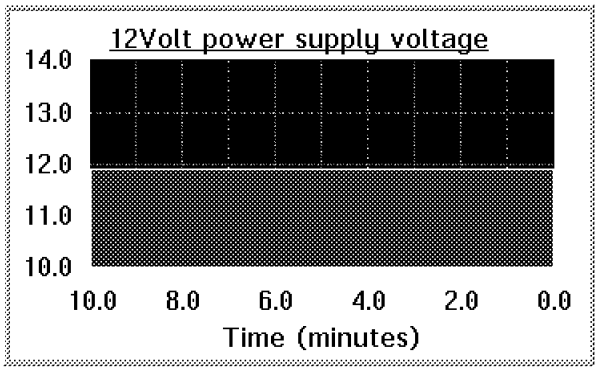


Figure 267. 12Volt Power Supply Voltage Monitor - Line Graph

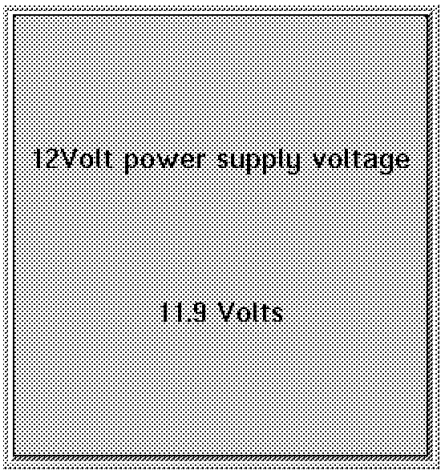


Figure 268. 12Volt Power Supply Voltage Monitor - Text Display

5.8.5 ServerGuard Adapter: Battery Voltage

The Battery voltage monitors follow:

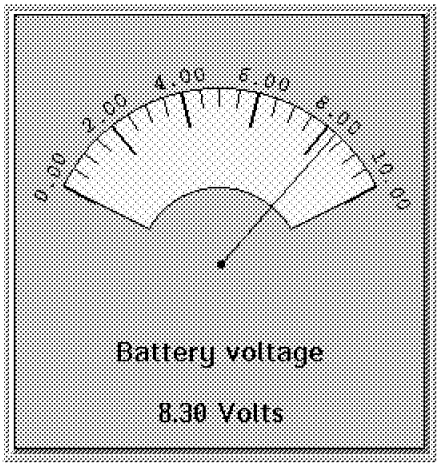


Figure 269. Battery Voltage Monitor - Real Time

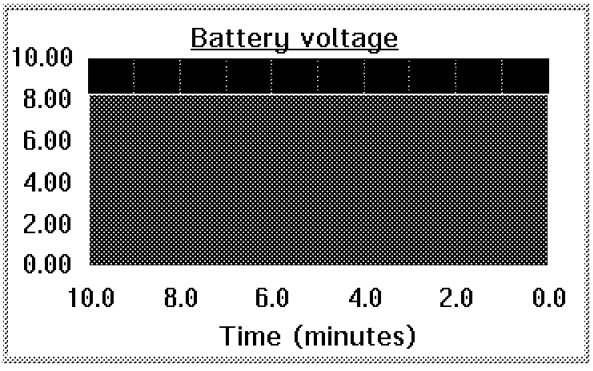


Figure 270. Battery Voltage Monitor - Line Graph

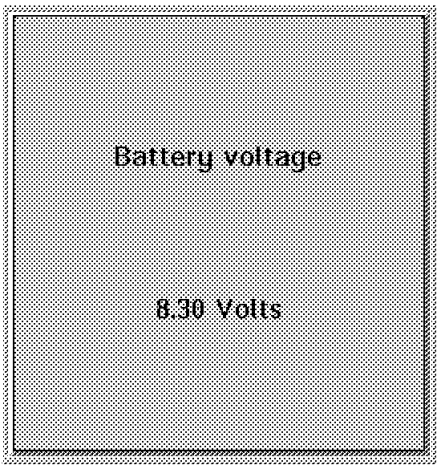


Figure 271. Battery Voltage Monitor - Text Display

5.8.6 ECC Memory

The ECC Memory monitors follow:

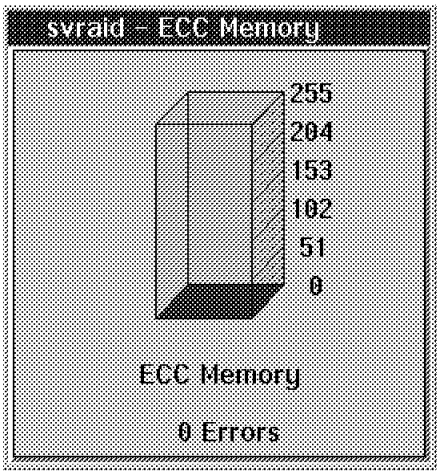


Figure 272. ECC Memory Monitor - Real Time

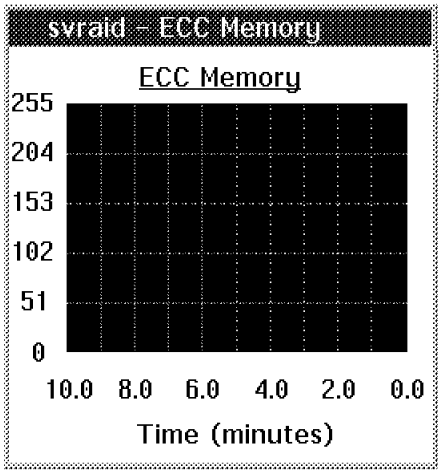


Figure 273. ECC Memory Monitor - Line Graph

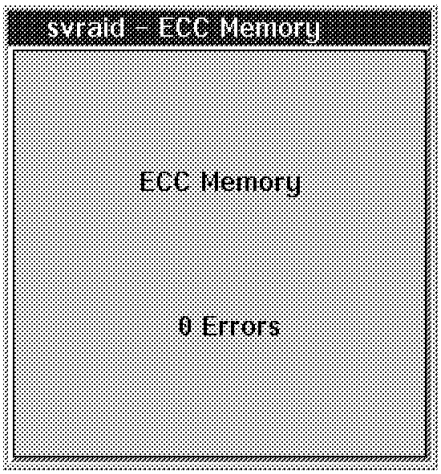


Figure 274. ECC Memory Monitor - Text Display

5.8.7 Pentium Processor: CPU Cache Hit Rate

The CPU Cache Hit Rate monitors follow:

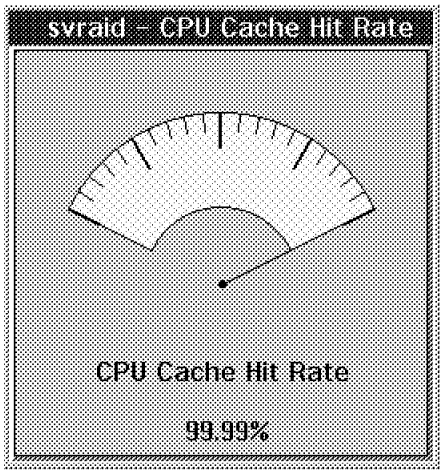


Figure 275. CPU Cache Hit Rate Monitor - Real Time

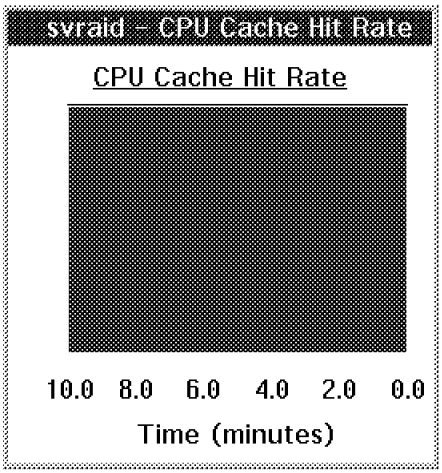


Figure 276. CPU Cache Hit Rate Monitor - Line Graph

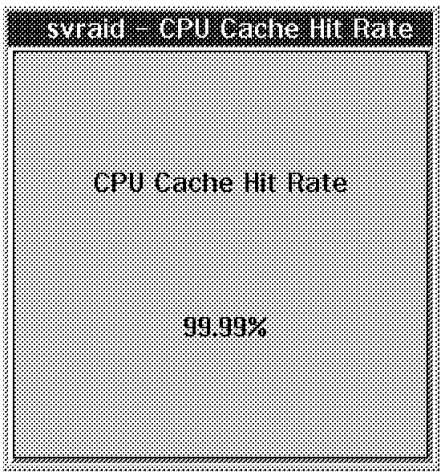


Figure 277. CPU Cache Hit Rate Monitor - Text Display

5.8.8 Pentium Processor: Memory I/O Rate

The Memory I/O Rate monitors follow:

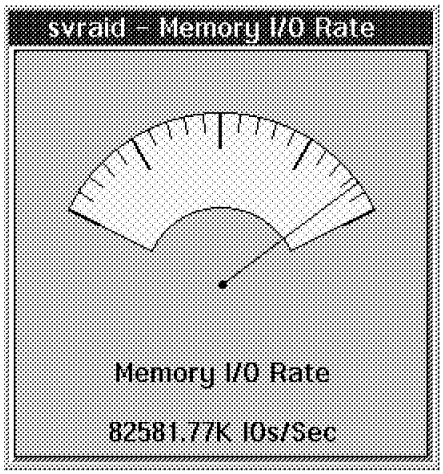


Figure 278. Memory I/O Rate Monitor - Real Time

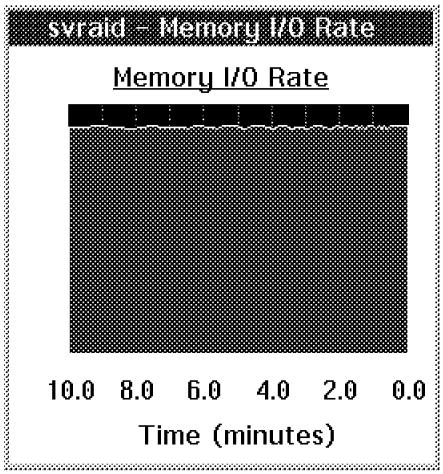


Figure 279. Memory I/O Rate Monitor - Line Graph

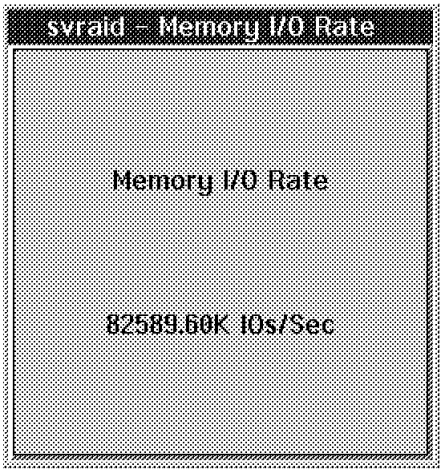


Figure 280. Memory I/O Rate Monitor - Text Display

5.8.9 Pentium Processor: Port I/O Rate

The Port I/O Rate monitors follow:

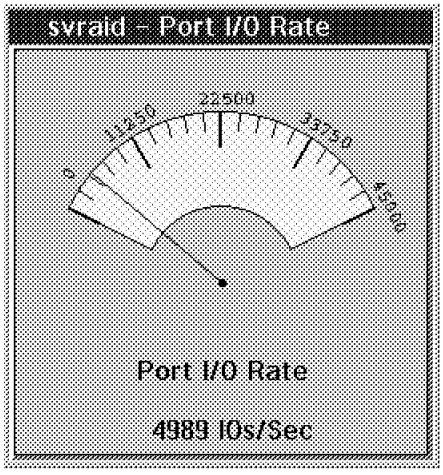


Figure 281. Port I/O Rate Monitor - Real Time

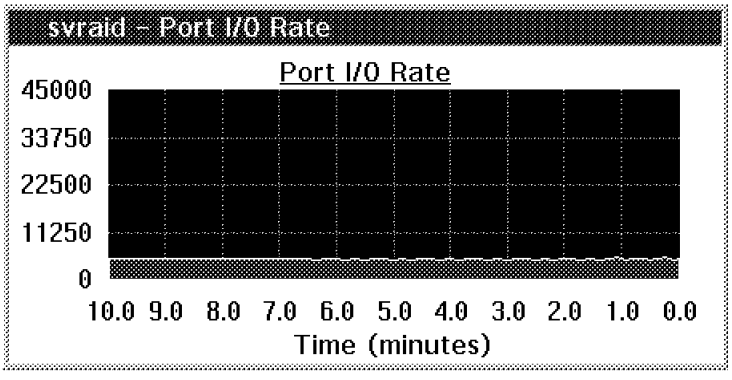


Figure 282. Port I/O Rate Monitor - Line Graph

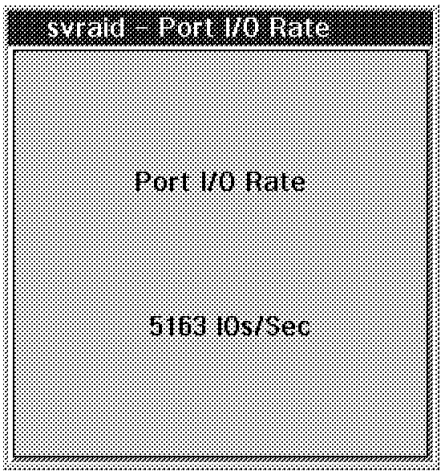


Figure 283. Port I/O Rate Monitor - Text Display

5.8.10 Pentium Processor: Interrupt Rate

The Interrupt Rate monitors follow:

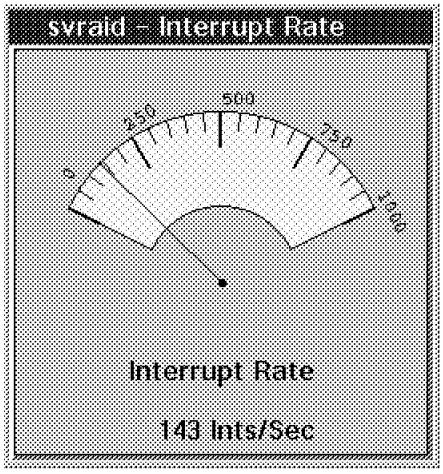


Figure 284. Interrupt Rate Monitor - Real Time

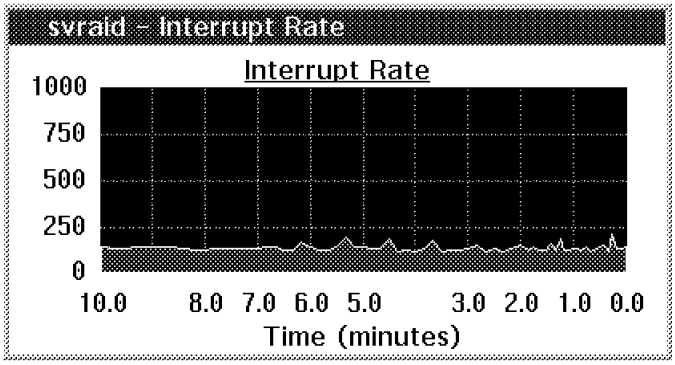


Figure 285. Interrupt Rate Monitor - Line Graph

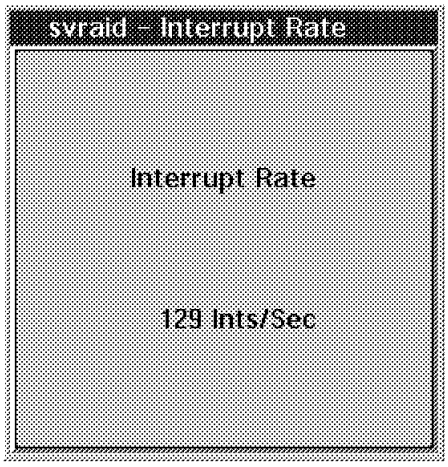


Figure 286. Interrupt Rate Monitor - Text Display

5.8.11 Pentium Processor: Floating Points Operation Rate

The Floating Points Operation Rate monitors follow:

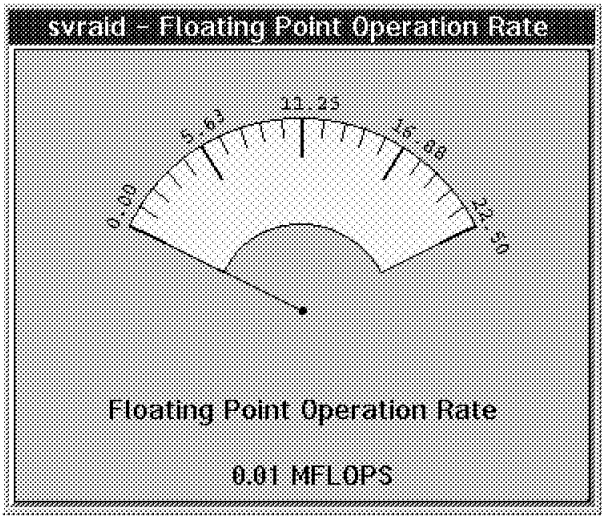


Figure 287. Floating Points Operation Rate Monitor - Real Time

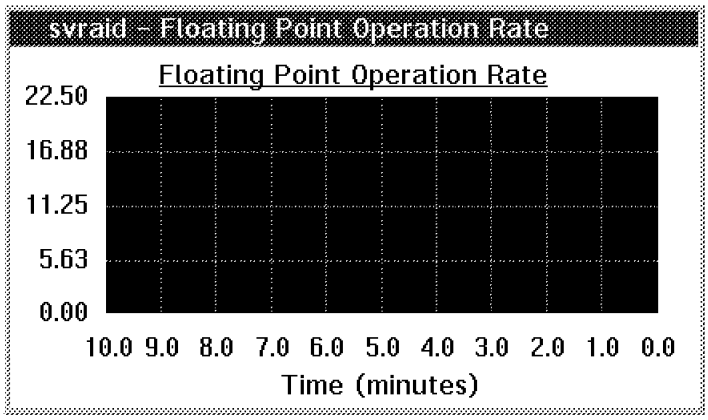


Figure 288. Floating Points Operation Rate Monitor - Line Graph

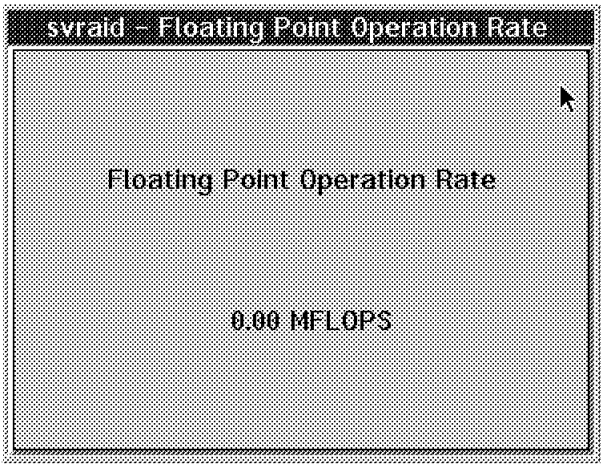


Figure 289. Floating Points Operation Rate Monitor - Text Display

5.8.12 Pentium Processor: Integer Instructions Rate

The Integer Instructions Rate monitors follow:

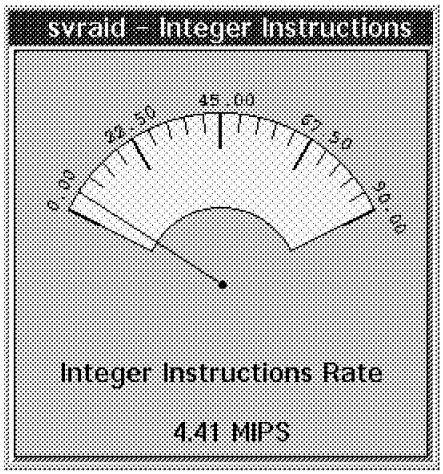


Figure 290. Integer Instructions Rate Monitor - Real Time

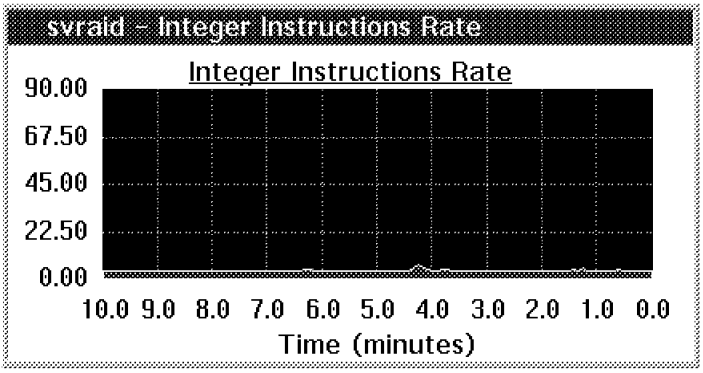


Figure 291. Integer Instructions Rate Monitor - Line Graph

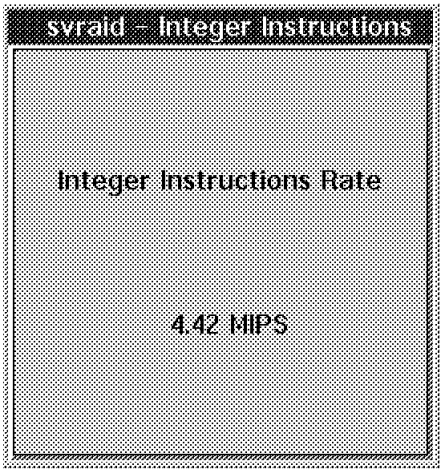


Figure 292. Integer Instructions Rate Monitor - Text Display

5.8.13 RAID Array

The RAID Array monitor is something special. It looks as follow:

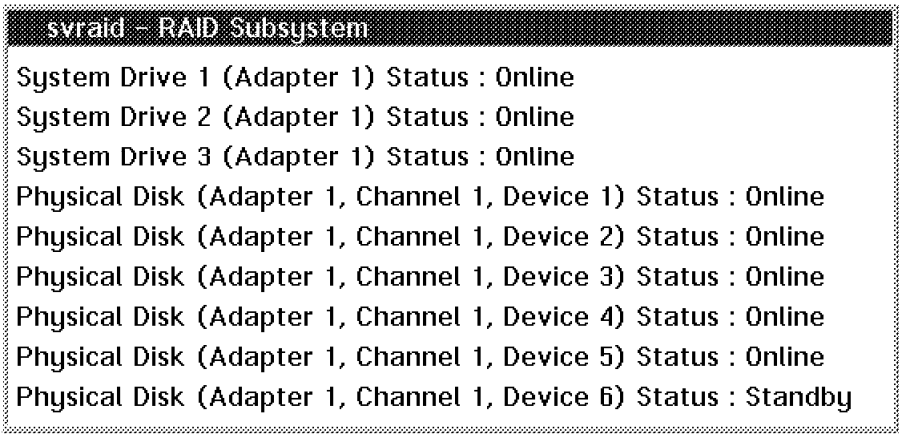


Figure 293. RAID Array Monitor

The RAID Array monitor has a set of switches, which indicate the current status of the RAID Array.

5.8.13.1 The RAID Monitor′s Pull-Down Menu

The RAID Monitor is displayed differently from the other monitors. The following figure shows an example of this:

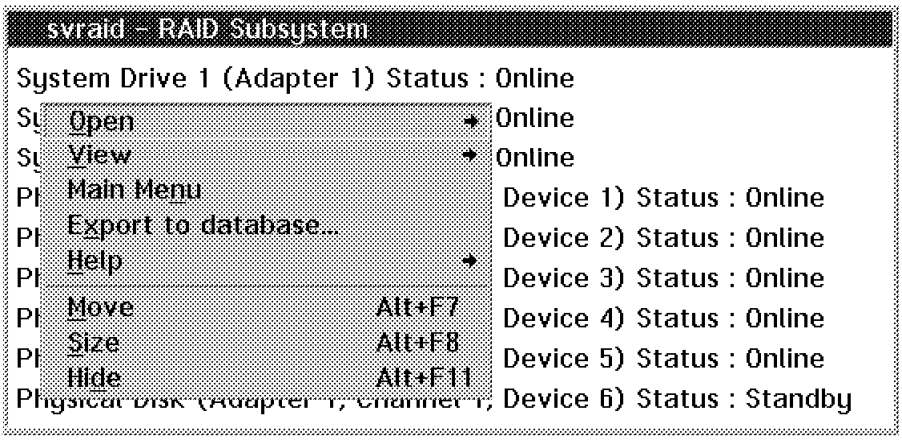


Figure 294. Pull-Down of the RAID Array Monitor

The RAID Monitors pull-down doesn′t have a view-selection available. That′s logical because there are no views available.

Clicking on **Open** → gives you the opportunity to open the Thresholds and the Settings of the RAID Monitor′s Notebook.

5.8.13.2 The RAID Monitor Notebook′s Settings

The RAID Monitor Notebook′s Settings follow:

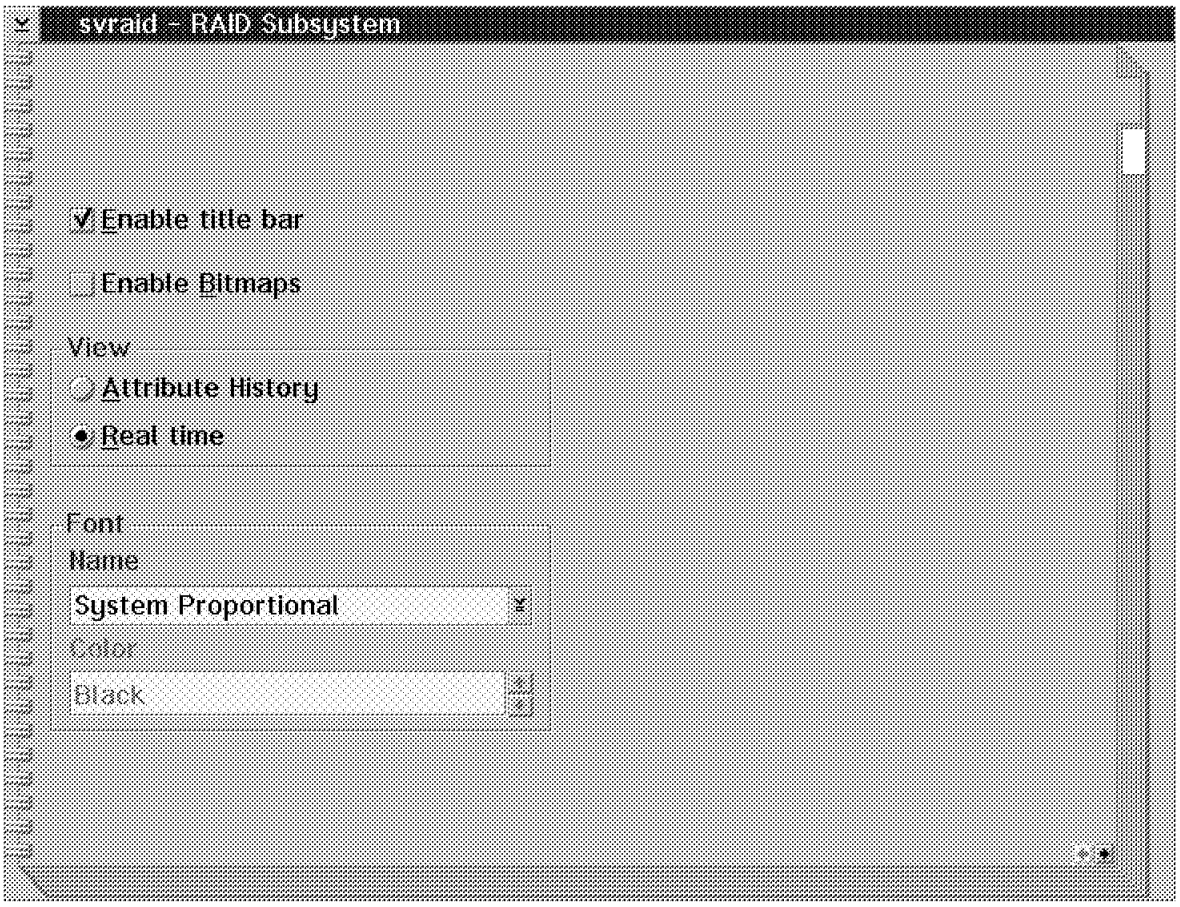


Figure 295. Settings for the RAID Array Monitor's Notebook

The settings are different then the other monitors, since the changes can only be done for the given text instead of data values.

5.8.13.3 The RAID Monitor Notebook's Thresholds

The RAID Monitor notebook thresholds follow:

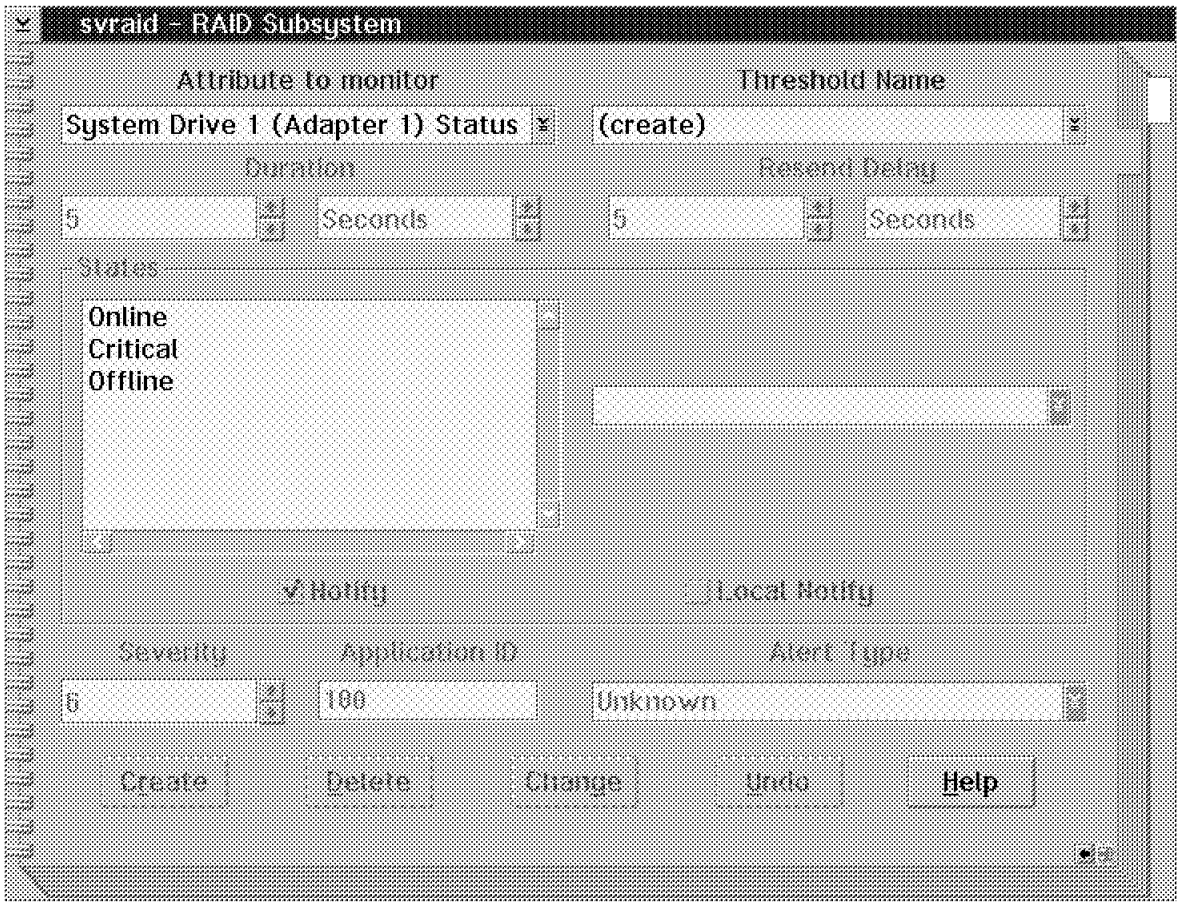


Figure 296. Thresholds of the RAID Array Monitor's Notebook

The threshold definition for the RAID Monitor is different from the ones used for all of the other notebooks. The threshold definition for the RAID array works as follows:

- The Attribute to monitor selection refers to the different attributes of the RAID monitor.

  You can set thresholds for all of the attributes available.

- In the Threshold Name selection you can define a threshold name for the threshold you are about to define.

  If you click on the down arrow, you get a list of pre-defined thresholds names you can activate.

- The States selection shows you all of the valid states for the current attribute.

  The state you select determines the event that will appear in any alerts that are sent.

- The other selections have the same meaning as they have in a default System monitor's notebook (see 5.3.2.2, "The Monitors Notebook Thresholds" on page 123).

Chapter 6. Serial Connections

This chapter deals with automated and semi-automated actions. This scenario will start the automatic problem file by doing the following:

- Issue a genalert to initiate the problem process.
- Establish the serial connection to the SystemView Manager.
- After connecting to the remote manager, initiate an exec to send information back to the manager on the problem.
- When the problem is resolved, have the manager issue an alert to contact remote client to disconnect.

Two workstations will report problems to the SystemView Manager, a Windows 95 workstation and an OS/2 workstation. The OS/2 workstation can have this scenario fully automated. On the Windows 95 workstation, operator intervention to start the serial connection will be required.

6.1 Customizing Serial Communication

First, we must make sure that the required hardware is installed. You should have at least one modem capable of operating at 9600 baud minimum on each machine. If possible, test the modems prior to starting the scenario with any local function your Operating System may provide. For example, on Windows 95, configure your modem in the Control Panel and try to dial out using the Phone Dialer provided. On OS/2, use the HyperAccess Lite provided with the BonusPak. These tests will help validate that any problems that occur when reproducing this scenario are not hardware related.

We already had the SystemView for OS/2 services module installed as Active Clients on each machine, as well as the SystemView Manager code on the OS/2 Manager. We also had NetFinity clients. Figure 297 on page 170 shows the screen to configure the serial communications driver. You will have to restart NETFBASE in SystemView for OS/2 after you make any changes to the configuration notebook.

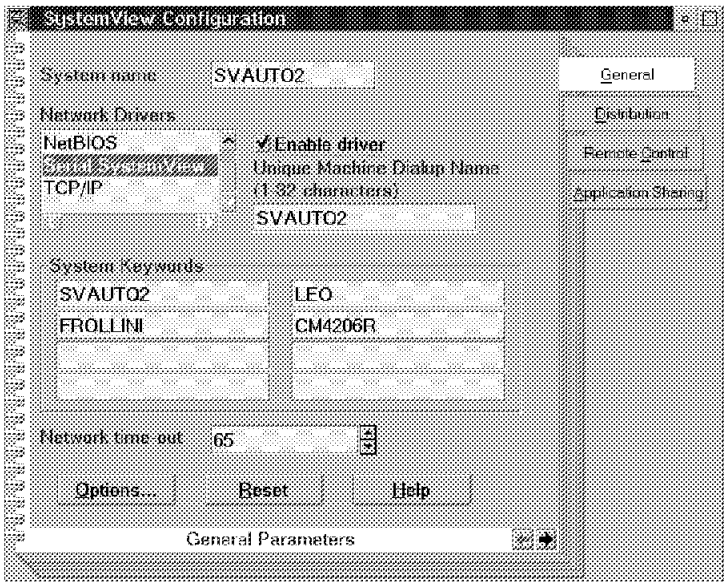


Figure 297. SystemView Configuration Notebook

On the General page, select **Serial SystemView under Network Drivers** and check the **Enable driver** check box to the right side. Enter the name you want the SystemView Manager to use to identify this machine under the Unique Machine Dial-up Name field. Then close the window which will save the new options in the configuration notebook.

Perform the same customization on the Windows 95 machine but under the NetFinity Network Driver Configuration program. Remember to shut down and restart NETFBASE in each machine to enable these changes.

The above customization will make SystemView for OS/2 and NetFinity start the module SERBASE.EXE every time the Services program is started. SERBASE.EXE will be mentioned again later in the scenario.

Serial Connections must always use User IDs and Passwords to verify access. Make sure you have at least one additional User ID defined in the Security Manager other than the default <PUBLIC> User ID. The default <PUBLIC> User ID is not valid for serial connections. We set up an user ID of Serial, with password XXXX for our serial connections.

Now start the SystemView Services GUI and select Serial Control. The following window will be displayed:

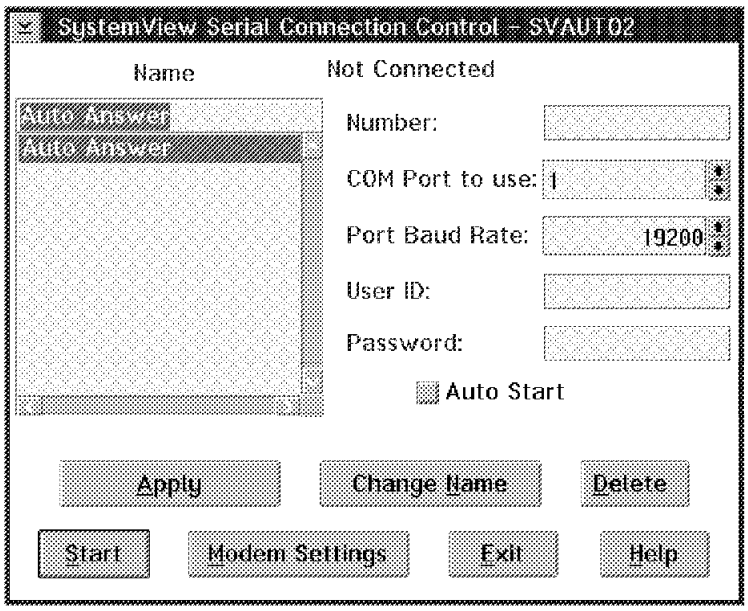


Figure 298. SystemView Serial Connection Control Window

Serial Control may be customized to automatically answer incoming calls or to call other workstations. Under this scenario, the client machine will contact the manager machine when an error is detected, so there must be an entry to call the manager on each client machine as well as an entry to automatically answer incoming calls on the manager machine.

Enter the connection name in the Name field. We used Manager on our machines. In the Number field, type in the phone number the SystemView Manager′s modem is attached to. Specify which COM port your modem is using in the *Comm Port to use* field, and what speed you will communicate at in the Port Baud Rate field. SystemView supports speeds starting at 9600 Baud.

Remember

If you need to dial a prefix before the actual phone number, remember to include it.

Enter the user ID and password in their respective fields. The Auto Start check box under the Password field will make SystemView automatically start this specific serial connection when NETFBASE is started. Do *not* check this check box at this time.

Now select **Modem Settings** to configure SystemView to your specific modem. The following window will appear:

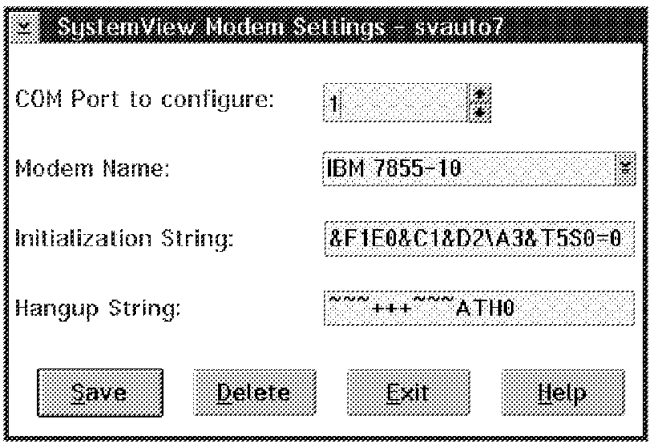


Figure 299. SystemView Modem Settings Window

Specify your modem settings in this window. Select your COM port, and your modem from the Modem Name list. This list is not very extensive. If you do not find your modem listed, a default modem entry is provided and should work with most Hayes compatible modems. After you select a modem name, the Initialization String and Hang-up String fields are filled in. These strings may not be correct for every modem in the modem list. The initialization string must configure the modem forthe following:

- Command echoing OFF
- Online character echoing OFF
- Result codes ENABLED
- Verbal result codes ENABLED
- All codes and connect messages with BUSY and DT detection
- Protocol identifier added - LAPM/MNP/NONE/V42bis/MNP5
- Normal CD operations
- DTR ON-OFF hang-up, disable AA, and return to command mode
- CTS hardware flow control
- RTS control of receive data to computer
- Queued and nondestructive break, no escape state
- Auto-answer off

Your modem documentation should provide detailed commands for each of these conditions. We used IBM 7855-10 modems and no changes to the parameters were necessary. After making the selections, select **Save** and **Exit**.

Back on the Serial Connection Control window, select **Apply** to make the changes valid. Select **Apply** and update the SERCALL.DAT file, used by SERBASE.EXE to establish the serial connections. We will look at SERCALL.DAT again in this chapter.

Perform the same customization steps on the two clients. On the Manager, perform the customization for an Auto Answer connection only. In this case, it is not necessary to fill in the Name, User ID and Password fields. After this customization, you are ready to start using your serial connection.

Use the status field in Figure 298 on page 171 to keep track of your serial connection status. The status field is to the right of the Name field, and above the Number field. If you have not started the serial connection, it should show Not Connected as it does in the following figure.

First start the Manager serial connection using the Start button as is shown in Figure 298 on page 171. If you are using an external modem, you should see a flickering of the lights on the modem. Depending upon the modem type, you may see the xx and yy lights lit up and the light on for the *Waiting for calls*. You should now test you client connections. After selecting the Manager connection name in the client′s Serial Control window, select **Start**. You should hear the modem dialing after a few seconds and the connection being established. The status will be shown in the status field. For example, dialing... connecting... and connected. When the connected status is shown on both the manager and the client, go to the Remote System Manager on the SystemView Manager and start the discovery process in any group you have created. Remember that the keyword names are case sensitive. Serial discovery takes a little longer, but your serial connected machine will show up and be available to be managed.

Select **Stop** on the client Serial Connection Control window to end the communication. You should see the status field go back to the Not Connected state after a few seconds, and the Manager state go back to Waiting for calls.

Important Note

If you use the SystemView DOS/Windows client in this scenario, be sure to close any serial connections that are currently active before closing the Program Manager. If you do not do this, the modem will not disconnect from the remote system.

6.2 Customizing Automation Routines

The automation routines will enable the client workstations to start the serial communication previously configured, send an alert to the managing station, and wait until an alert or command is sent signaling *end-of-diagnosis*.

6.2.1 Automated Dialing from the OS/2 Workstation

The OS/2 workstation has been customized with an entry to call the SystemView Manager manually. The file SERCALL.DAT on the SystemView directory contains this manual configuration. Save it into the file SERCALL.MAN using the following command:

```
COPY SERCALL.DAT SERCALL.MAN
```

Go back to the Serial Connection Control window (Figure 298 on page 171), select the Manager connection name and now click on **check the Auto Start** check box. Select **Apply**, then **Exit**. This will update the SERCALL.DAT file to automatically start the communication to the SystemView Manager when the serial base program SERBASE.EXE is started. Save the *new* SERCALL.DAT into the file SERCALL.AUT.

```
COPY SERCALL.DAT SERCALL.AUT
```

Now you have the following two configuration files for serial communications:

- SERCALL.MAN contains customization for manual connections
- SERCALL.AUT contains customization for automatic connections

When the problem is detected in our automated process, we will copy the automatic customization to SERCALL.DAT and restart the serial base. This will cause SystemView to automatically dial up the manager and send the alert documenting the problem.

We will use one control file to check if the serial connection is up or not. The file SERIAL.ON will indicate the connection is up. When the connection is brought down, this file will be deleted. Therefore, all processes will first check for the existence of SERIAL.ON prior to carrying out startup or shutdown of the serial connection. This can be done with a simple REXX EXEC.

The CNCT.CMD program below starts the serial connection and generates an alert. All alert parameters *must* be passed to the program in order to generate the alert to be forwarded to the manager. The Alert Manager must be previously set to forward the alert using the SERIAL protocol to the SystemView Manager. The serial connection will be left up until the DISCNCT.CMD program is executed to terminate the connection.

```
/* REXX for OS/2                                                    */
/*                                                                  */
/* Procedure to start serial connection                             */
/*                                                                  */
/* MANAGER must be in Auto Answer mode                              */
/*                                                                  */

'@ECHO OFF'    /* Load REXX Functions  */
Trace Off
Call RxFuncAdd "SysLoadFuncs","RexxUtil","SysLoadFuncs"
Call SysLoadFuncs

If Arg() = 0
   Then Call NoParms               /* Error if no parameters            */

SerialOn   = 'SERIAL.ON'           /* Serial Connection Status File Name */
SysViewDir = 'D:\SYSVIEW2\BIN'     /* If you dont know where SysView is, */
CurrentDir = Directory(SysViewDir) /* write procedure to find it...      */
ChgFile.   = ' '
ChgFile.0  = 2
ChgFile.1  = 'SERCALL.MAN'         /* File for Manual Connection         */
ChgFile.2  = 'SERCALL.AUT'         /* File for Auto Call Manager         */

rc = SysFileTree(SerialOn,IsThere,'F')

If IsThere.0 > 0
   Then do
        Say 'Serial Connection already up.'
        Say 'Call DISCNCT.CMD before running this program.'
        Exit
        end

Call FindSERBASE                    /* Call to find and kill serbase */
NewSERCALL = ChgFile.2              /* Set serbase file              */
Call ChangeSERCALL                  /* Call to copy new over current */

Arg TIM DAT SEV SND APP AT TypeAndText     /* Process Parameters     */

Parse Upper Var TypeAndText '"' Type '" "' TXT '"'

Select
  When Pos('OPERATING',Type)   <> 0 Then TYP1 = 'OS_'
  When Pos('SYSTEM',Type)      <> 0 Then TYP1 = 'SYS'
  When Pos('DASD',Type)        <> 0 Then TYP1 = 'DSK'
  When Pos('APPLICATION',Type) <> 0 Then TYP1 = 'APP'
  When Pos('DEVICE',Type)      <> 0 Then TYP1 = 'DEV'
  When Pos('SECURITY',Type)    <> 0 Then TYP1 = 'SEC'
  Otherwise                         TYP1 = 'UNK'
End

Select
  When Pos('FAULT',Type)       <> 0 Then TYP2 = 'FLT'
  When Pos('ERROR',Type)       <> 0 Then TYP2 = 'ERR'
  When Pos('WARNING',Type)     <> 0 Then TYP2 = 'WRN'
  When Pos('INFORMATION',Type) <> 0 Then TYP2 = 'INF'
  Otherwise                         TYP2 = 'UNK'
End

Say "START /C /MIN " CurrentDir||"\SERBASE "
    "START /C /MIN " CurrentDir||"\SERBASE "

Say "Waiting for SERIAL CONNECTION"
Call SysSleep 25

Call CreateStatusFile

Say 'GENALERT /T:"'TXT,
       '" /APP:'APP,
         '/SEV:'SEV,
         '/TYPE:'TYP1||TYP2,
         '/ATYPE:'AT
/*       '/N:SERIPC::MGRNAME' Uncomment if your version of GENALERT supports /N: */

'GENALERT /T:"'TXT,
       '" /APP:'APP,
         '/SEV:'SEV,
         '/TYPE:'TYP1||TYP2,
         '/ATYPE:'AT
/*       '/N:SERIPC::MGRNAME' Uncomment if your version of GENALERT supports /N: */

Exit
```

```
/*  This procedure uses some IBM INTERNAL routines from the OS2TOOLS repository.   */
/*  REAL CUSTOMERS can not have these routines. Customer MUST write ther own      */
/*  routine to FIND the PROCESS ID of SERBASE then Kill it.                        */

/*  WARNING:: This routine can not determine if you really want to kill the  */
/*  connection or not. The procedure KILLs serbase regardless of whom may be using it */
/*  KILLs serbase without regards to who may be using it.                          */

FindSERBASE: procedure        /* Find and Kill SERBASE         */
'Call PS > C:\SERBASE.TMP'    /* PS is an IBM Internal routine */
 rc = SysFileSearch('serbase','c:\serbase.tmp',lines)
 if (rc \= 0) | (lines.0 > 1) then
    do
       rc = SysFileDelete('c:\serbase.tmp')
       not_found = 'Could not find SERBASE'
       return (not_found)
    end
 else if lines.0 = 1 then
    do
       parse var lines.1 procid lines.1
       'Call kill 'procid            /* KILL is an IBM Internal routine */
        Call SysSleep 3
       'Call PS > c:\serbase.tmp'    /* PS is an IBM Internal routine   */
       rc = SysFileSearch('serbase','c:\serbase.tmp',lines)
       if lines.0 \= 0 then
          do
             rc = SysFileDelete('c:\serbase.tmp')
             not_dead = 'SERBASE not KILLED'
             return (not_dead)
          end
    end

 rc = SysFileDelete('c:\serbase.tmp')
 Return (0)

/* Procedure for Creating Status file  */

CreateStatusFile: procedure expose CurrentDir
'Call copy' CurrentDir||'\SERCALL.DAT' CurrentDir'\SERIAL.ON'
 Return (0)

/* Procedure for Changing .DAT files from automatic dialing to manual */

ChangeSERCALL: procedure expose NewSERCALL CurrentDir
'Call copy' CurrentDir||'\'NewSERCALL CurrentDir'\sercall.dat'
 Return (0)

NoParms: procedure
Say 'Please provide the following parameters from the Action Editor:'
Say '  Time'
Say '  Date'
Say '  Severity'
Say '  Sender'
Say '  Application'
Say '  Application Alert Type'
Say '  Alert Type'
Say '  Alert Text'
Exit (999);
```

Figure 300 (Part 2 of 2). CNCT.CMD Sample OS/2 REXX Program to Connect Using a Modem and Send an Alert

```
/* REXX for OS/2                                                */
/*                                                              */
/* Procedure to stop serial connection                          */
/*                                                              */

'@ECHO OFF'                            /* Load REXX Functions */
Trace Off
Call RxFuncAdd "SysLoadFuncs","RexxUtil","SysLoadFuncs"
Call SysLoadFuncs

SerialOn   = 'SERIAL.ON'           /* Serial Connection Status File Name */
SysViewDir = 'D:\SYSVIEW2\BIN'     /* If you dont know where SysView is, */
CurrentDir = Directory(SysViewDir) /* write procedure to find it...      */
ChgFile.   = ' '
ChgFile.0  = 2
ChgFile.1  = 'SERCALL.MAN'         /* File for Manual Connection         */
ChgFile.2  = 'SERCALL.AUT'         /* File for Auto Call Manager         */

rc = SysFileTree(SerialOn,IsThere,'F')

If IsThere.0 = 0
   Then do
        Say 'Serial Connection already down.'
        Exit
        end

Call FindSERBASE                /* Return sercall to original state */
NewSERCALL = ChgFile.1
Call ChangeSERCALL

Say "START /C /MIN " CurrentDir||"\SERBASE"
    "START /C /MIN " CurrentDir||"\SERBASE"

Exit

/*                                                                                  */
/*  This procedure uses some IBM INTERNAL routines from the OS/2TOOLS               */
/*  repository. REAL CUSTOMERS can not have these routines. Customer                */
/*  MUST write their own routine to FIND the PROCESS ID if SERBASE and then kill it */
/*                                                                                  */

/*  WARNING:: This routine can not determine if you really want to kill the connection */
/*  or not. The procedure KILLs serbase without regards to who may be using it        */

FindSERBASE: procedure        /* Find and Kill SERBASE         */
'Call PS > C:\SERBASE.TMP'    /* PS is an IBM Internal routine */
 rc = SysFileSearch('serbase','c:\serbase.tmp',lines)
 if (rc \= 0) | (lines.0 > 1) then
    do
       rc = SysFileDelete('c:\serbase.tmp')
       not_found = 'Could not find SERBASE'
       return (not_found)
    end
 else if lines.0 = 1 then
    do
       parse var lines.1 procid lines.1
       'Call kill 'procid            /* KILL is an IBM Internal routine */
        Call SysSleep 3
       'Call PS > c:\serbase.tmp'    /* PS is an IBM Internal routine   */
       rc = SysFileSearch('serbase','c:\serbase.tmp',lines)
       if lines.0 \= 0 then
          do
             rc = SysFileDelete('c:\serbase.tmp')
             not_dead = 'SERBASE not KILLED'
             return (not_dead)
          end
    end

 rc = SysFileDelete('c:\serbase.tmp')
 Return (0)

/* Procedure for Changing .DAT files   */
/* from Automatic dialing to Manual    */

ChangeSERCALL: procedure expose NewSERCALL CurrentDir
'Call copy' CurrentDir||'\'NewSERCALL CurrentDir'\sercall.dat'
 Return (0)
```

Figure 301. DISCNCT.CMD Sample OS/2 REXX Program to Stop Modem Connections

6.2.2 Dialing from the Windows 95 Workstation

The process on the Windows 95 workstation is semi-automated since we did not have a tool to perform a list and then kill a process from a command line. If you have your own tool to do that, you can fully automate this process.

When the problem is detected, the alert will trigger a pop-up window and the Serial Connection Control window asking the user to select **Start** to start the serial connection. After the problem is resolved, another pop-up will prompt the user to stop the serial connection.

We will use the LMPOPUPW.EXE module from LAN NetView Management Utilities for OS/2 (LMU) to issue the pop-up window. Use any tool to perform this function if you do not have LMU available.

```
/* REXX for DOS                                      */
/*                                                   */
/* Procedure to start serial connection              */
/*                                                   */
/* MANAGER must be in Auto Answer mode               */
/*                                                   */

'@ECHO OFF'    /* Load REXX Functions  */
Trace off

If Arg() = 0
   Then Call NoParms               /* Error if no parameters            */

SerialOn   = 'SERIAL.ON'           /* Serial Connection Status File Name */
SysViewDrv = 'C:'
SysViewDir = 'C:\WNETFIN'          /* If you dont know where SysView is, */
rc         = RxChDrv(SysViewDrv)   /* write procedure to find it...      */
rc         = RxChDir(SysViewDir)
LmuMsg     = 'Select OK. Press START, then EXIT on the Serial Connection',
             'Control Window to connect to SystemView Manager.'
IdealLmuMsg = 'Error Detected. Automatic Recovery Started. Please',
             'select OK on this window and press START on the Serial Connection',
             'Control Window do begin connection with the SystemView Manager.'

IsThere = RxFInfo(SerialOn)

If IsThere <> ''
   Then do
        Say 'Serial Connection already up.'
        Say 'Call DISCNCT.CMD before running this program.'
        Exit
        end

'SERGUI'
rc = RxSleep(1) /* change value according to workstation's resp time */
'LMUPOPW "'lmumsg'"'
rc = RxSleep(60)

Arg TIM DAT SEV SND APP AT TypeAndText     /* Process Parameters     */

Divide = Pos('" "',TypeAndText)            /* Separate Type and Text */
TYP1   = SubStr(TypeAndText,2,Divide-2)
TYP2   = SubStr(TypeAndText,Divide+3,Length(TypeAndText)-1)

Select
  When Pos('OPERATING',TYP1)   <> 0 Then TYP1 = 'OS_'
  When Pos('SYSTEM',TYP1)      <> 0 Then TYP1 = 'SYS'
  When Pos('DASD',TYP1)        <> 0 Then TYP1 = 'DSK'
  When Pos('APPLICATION',TYP1) <> 0 Then TYP1 = 'APP'
  When Pos('DEVICE',TYP1)      <> 0 Then TYP1 = 'DEV'
  When Pos('SECURITY',TYP1)    <> 0 Then TYP1 = 'SEC'
  Otherwise                         TYP1 = 'UNK'
End

Select
  When Pos('FAULT',TYP2)       <> 0 Then TYP2 = 'FLT'
  When Pos('ERROR',TYP2)       <> 0 Then TYP2 = 'ERR'
  When Pos('WARNING',TYP2)     <> 0 Then TYP2 = 'WRN'
  When Pos('INFORMATION',TYP2) <> 0 Then TYP2 = 'INF'
  Otherwise                         TYP2 = 'UNK'
End

Say "Waiting for SERIAL CONNECTION"
Call SysSleep 25

Call CreateStatusFile

Say 'GENALERT /T:" ' TXT ,
      ' " /APP:'APP ,
         '/SEV:'SEV ,
         '/TYPE:'TYP1||TYP2 ,
         '/ATYPE:'AT
/*       '/N:SERIPC::MGRNAME' Uncomment if your version of GENALERT supports /N: */

'GENALERT /T:" ' TXT ,
      ' " /APP:'APP ,
         '/SEV:'SEV ,
         '/TYPE:'TYP1||TYP2 ,
         '/ATYPE:'AT
/*       '/N:SERIPC::MGRNAME' Uncomment if your version of GENALERT supports /N: */
```

```
Exit

/* Procedure for Creating Status file  */

CreateStatusFile: procedure expose SysViewDir
'Call copy' SysViewDir||'\SERCALL.DAT' SysViewDir'\SERIAL.ON'
 Return (0)

NoParms: procedure
Say 'Please provide the following parameters from the Action Editor:'
Say '  Time'
Say '  Date'
Say '  Severity'
Say '  Sender'
Say '  Application'
Say '  Application Alert Type'
Say '  Alert Type'
Say '  Alert Text'
Exit (999);
```

Figure 302 (Part 2 of 2). WCNCT.CMD Sample DOS REXX Program to Prompt User to Start Serial Communication

```
/* REXX for DOS                                      */
/*                                                   */
/* Procedure to stop serial connection               */

Trace off

SerialOn   = 'SERIAL.ON'           /* Serial Connection Status File Name */
SysViewDrv = 'C:'
SysViewDir = 'C:\WNETFIN'          /* If you dont know where SysView is, */
rc         = RxChDrv(SysViewDrv)   /* write procedure to find it...      */
rc         = RxChDir(SysViewDir)
LmuMsg     = 'Select OK. Press STOP, then EXIT on the Serial Connection',
             'Control Window to stop connection to SystemView Manager.'
IdealLmuMsg = 'Automatic Recovery finished. Please',
              'select OK on this window and press STOP on the Serial Connection',
              'Control Window do stop connection with the SystemView Manager.'

IsThere = RxFInfo(SerialOn)

If IsThere = ''
   Then do
        Say 'Serial Connection already down.'
        Exit
        end

'SERGUI'
/* rc = RxSleep(1) uncomment and chg value according to performance  */
'LMUPOPW "'lmumsg'"'

'Call delete ' SysViewDir||'\SERIAL.ON'

Exit
```

Figure 303. WDISCNCT.CMD Sample DOS REXX Program to Prompt User to Stop Serial Communication

Chapter 7. Creating Policies for New SystemView Clients

This chapter deals with the application of defined policies to new clients. The process to generate policies is explained here. This chapter has three main parts:

- Policy setup
- Package preparation
- Change file scheduling

7.1 Policy Setup

The configuration of any system running SystemView requires the following INI files. They can be found in the C:\SYSVIEW2\BIN directory.

- NETDRVR.INI
- KARAT.INI
- FNDSHARE.INI
- FNDSWOBJ.INI
- SVCMGR.INI
- DCAF.INI
- SVSHAPP.INI
- NETDOM.INI
- NETNODES
- NETMGR.INI
- SECOUT.INI
- SECIN.INI
- MONCRIF.INI
- MONTHR.INI
- MONDATA.INI
- ALACTION.INI
- SINVGUI.INI
- SHRIEKER.INI
- RAIDGUI.INI
- IKOSVC.INI
- NEWSERV.INI
- SVSHAPP.INI

You can only edit these files through the Services GUI for each component. You can not use a standard operating system editor to make any changes. For example, if you want to add a new file to the critical file monitor list from a client, you will have to:

- Obtain a copy and place it in your \SYSVIEW2\BIN directory.

- Double-click on the **Critical File Monitor Service**.
- Make your changes or additions to the file list.
- Save your changes.
- Send a copy of that INI file back to the client.

7.1.1 Descriptions of the INI Files

The following is a description of some of the INI files that are commonly used and will most likely be distributed to clients.

- NETDRVR - This file is modified each time you access the SystemView Configuration in the SystemView Folder. The information contained in this file follows:
  - System Name
  - Network Driver
    - NetBIOS
    - IPX
    - Serial
    - TCP/IP
  - System Keywords
- NETDOM - This file contains the information related to the existing groups in this system, if you add or remove a group, this file will be changed.
- SECOUT - This file contains those users who want to access remote systems. Every time you add a user, this file is modified.
- SECIN - This file contains those users who want to login and access this system.
- MONCRITF - This file is modified when you add a file to the Critical File list or change a value like severity for a file already in the list.
- MONTHR - This file is modified only if a threshold is established for any monitor. The information kept here is related to the name of the threshold.
- ALACTION - Contains the actions to be executed once the alarm criteria is reached. The description of the Action editor is shown in Figure 304 on page 183.

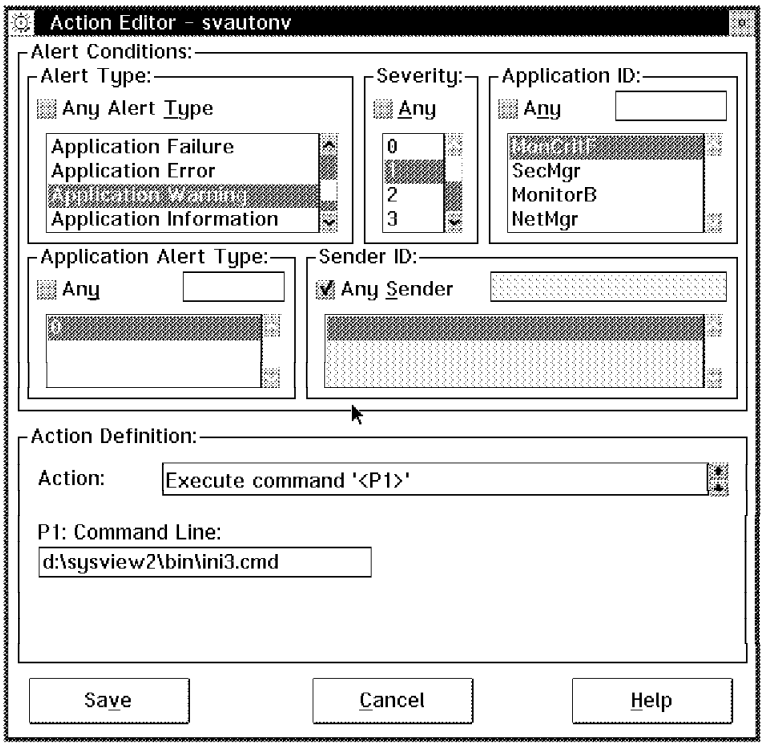


Figure 304. Action Editor

So let's suppose you have a group of 10 clients and you want to apply a common policy in order to maintain control, as well as providing a standard that will assist the help desk. One way would be to remotely logon to each system through the Remote Session Manager and start each service that you wish to modify and then make the same changes on each system. An easier and more efficient way would be to create all the INI control files on your Manager system and distribute them to all of your clients.

We selected the second approach and we combined that approach with the use of the Scheduler service to keep everything up to date.

Our standard model had the following characteristics:

- Each client should be able to forward any alert to the system WTR05261 using the NetBIOS protocol.
- The CONFIG.SYS and the STARTUP.CMD file should be marked as critical file in the critical file monitor.
- Only the ADMIN user ID should be allowed to logon to the clients.
- The threshold for the CPU utilization should be set at 60 percent.

In order to generate the proper INI files the following process was applied:

- Shutdown SystemView

  Rename the following files as extension BAK since we don't want to permanently change the managers INI files. We just want to set up the clients.

  – MONTHR.INI
  – MONCRITF.INI

  - ALACTION.INI
  - SECIN.INI
  - SECOUT.INI
- Initialize **SystemView**.
- Click on the **Alert Manager** icon.
- Click on **Actions**.
- Select **New**.
- Select all the buttons.
- Click on the action **Forward Alert to ....**.
- Select the protocol **NetBIOS**, and the name of the remote workstation as WTR05261.
- Click on **Save**.
- Click on **Done**.
- Close the icon.
- Click on the **Critical File Monitor** icon.
- Click on the **CONFIG.SYS** and **STARTUP.CMD** check boxes.
- Click on **Save**.
- Close the icon.
- Click on the **Security Manager** icon.
- Click on **Edit/Display Outgoing Passwords**.
- Click on **Add**.
- Type the user ID ADMIN and the password.
- Click on **Set**.
- Click on **Exit**.
- Close the icon.
- Click on the **System Monitor** icon.
- Click on **Windows**.
- Click on **Show**.
- Mark Monitor CPU Utilization.
- Click on **Accept**.
- In the CPU Utilization box press the right mouse button.
- Click on **Open**.
- Click On **Settings** and go to the second page.
- Type a new name, establish the minimum time to trigger an alarm and the severity.
- Type the percentage of usage that will be your threshold.
- Click on **create**.
- Close the Setup window.
- Shut down SystemView.

- Copy the new files to d:\repos. This subdirectory has to already exist.
- Rename the files extension BAK to INI.
- Initialize **SystemView**.

Once you have completed the above steps the model is ready. There are five new files in the path d:\repos. These files will be distributed to the remote systems. In order to do this you will have to prepare a Software package.

7.2 Package Preparation

The steps to prepare the package follow:

- Create the files to be transferred to the remote system.
- Create the scripts for pre-installing and for post installation.
- Create the variables to be used.

For this sample the files transferred were:

- d:\repos*.* with a destination of d:\initempo
- d:\pgms\maked.cmd with a destination of d:\
- d:\pgms\preini.cmd with a destination of d:\
- d:\pgms\shutd.cmd with a destination of d:\

Figure 305 shows the program preini.cmd. The program maked.cmd follows:

- md $(sv):\initempo
- copy $(sv):\preini.cmd $(siop):\desktop\ os!2 system \startup

The program shutd.cmd is only the shutdown command.

Figure 305. PREINI.CMD Program

The sequence is as follows:

1. The program maked.cmd will create a subdirectory d:\initempo and it will copy the file preini.cmd to the path c:\desktop\os!2 system\startup, in order to be executed during startup.
2. The files in d:\repos*.* are transferred to d:\initempo on the remote system.
3. The program shutd.ini is executed as a post installation script.

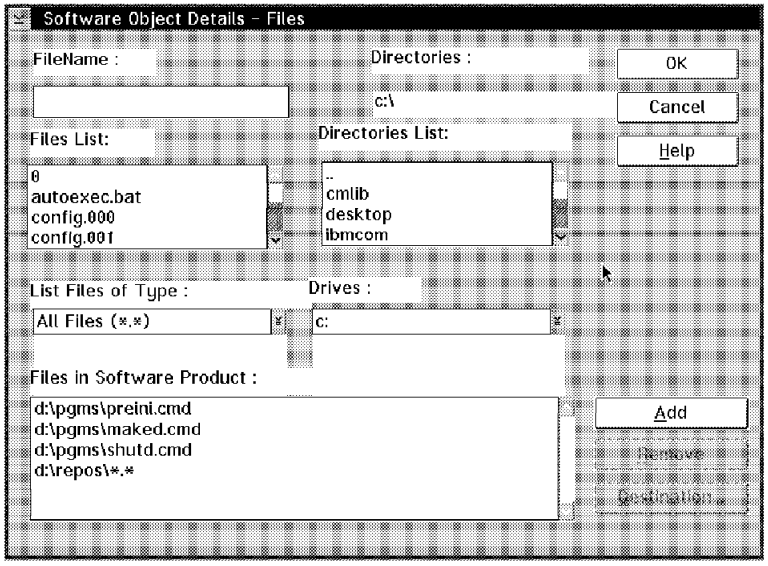


Figure 306. Object Details Files

The process to add this information has been explained in Chapter 4, “Automating Software Package Install” on page 77. Please refer to it in order to add the files. Figure 306 shows the files that have to be added. Figure 307 shows where to put each script. Finally, Figure 308 on page 187 contains the variables we used. These variables point to the logical drive in which you want to install the files. Make sure you change the values as soon as you get to the Software Preparation GUI. In order to change the value of these variables, you will need to do the following:

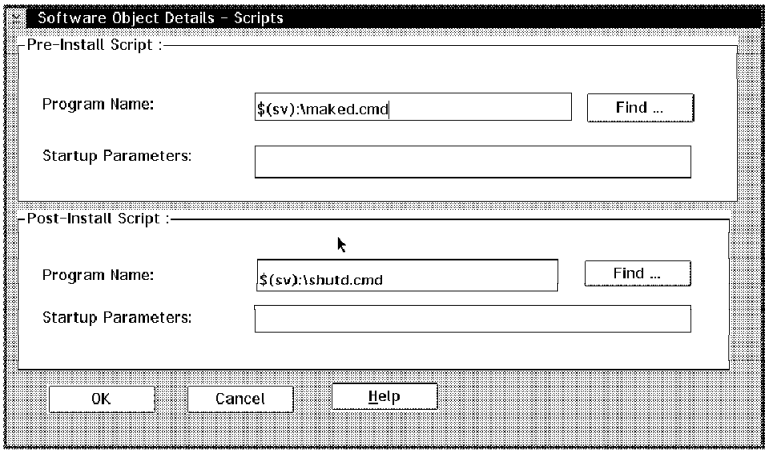


Figure 307. Files Destination

- Click on the **Software Preparation** icon.

- Click on **Software** and then **New**.
- From the new window, click on **Files**.
- Select the files that you just created.
- Add the destination for each file (Figure 309 shows the destination for one file).
- Once you have selected the files that are part of the change file, you can add the script for pre- and post-installation as shown in Figure 307 on page 186.
- In this sample we used some variables for the drives used to install the change files. These variables are specified in the **Variables** icon. Click on this icon and then type the name of the variable and its value. Then click on **set**.
- Close these windows, click on **Software** and then select **Catalog**. You may get an informational message indicating that the catalog process completed successfully.

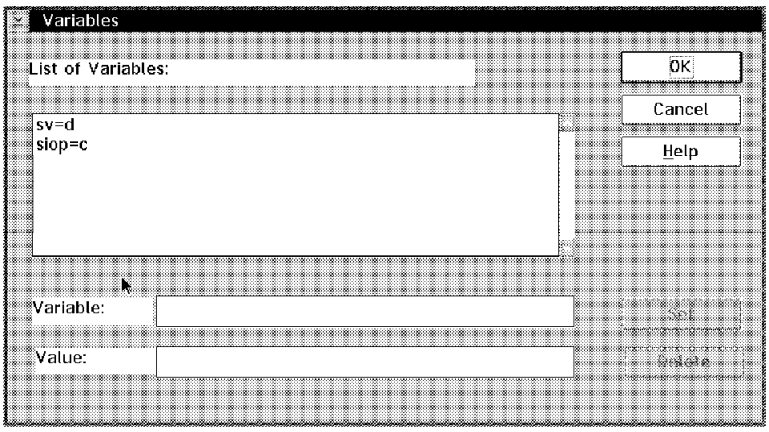


Figure 308. Object Details Variables

Once the package has been cataloged, it is ready to be distributed. For this sample we used the Scheduler service. The steps used for distribution are as shown in Figure 309.

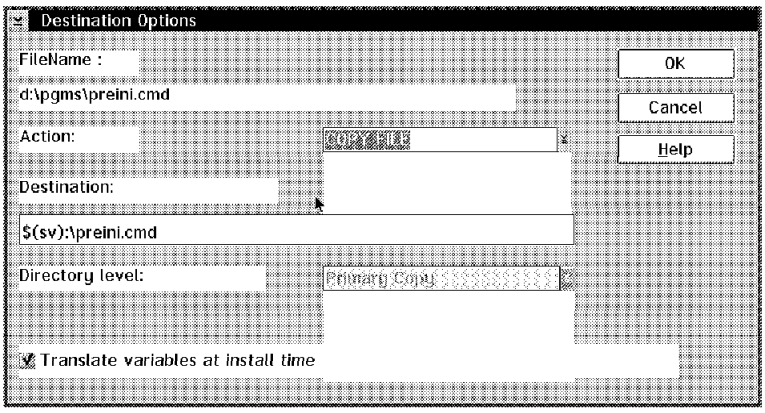


Figure 309. Destination Options

- Click on the **Scheduler Event** icon.

- Click on **New**.
- Type the name of the event (INI Update).
- Click on **Software Distribution**.
- Click on the **System** or **Group** button (depending upon if you are going to schedule it for one system, or a group of systems).
- Click on **Schedule**.
- A new window will pop up.
- Click on **Software Products**.
- From the new window, you should be able to see the name you already entered for the software package.
- Click on it and be sure that it is the only one marked.
- Click on **Software** and choose **Install**.
- A new window will let you select how you want to install this package. Choose **Ignore current status of Software Object**.
- Click on **Save**.
- A scheduler will come up using the options you wanted and fill in the correct fields.
- Click on **Save**.
- The event has been added to the scheduler and will be executed within one minute for the system(s) unless you changed the scheduler time.

In order to automate the process, a program to run the scheduler and the software preparation needs to be set up. This program can be executed as a result of a specific kind of alert received by the Alert Manager process. This program would look like Figure 310.

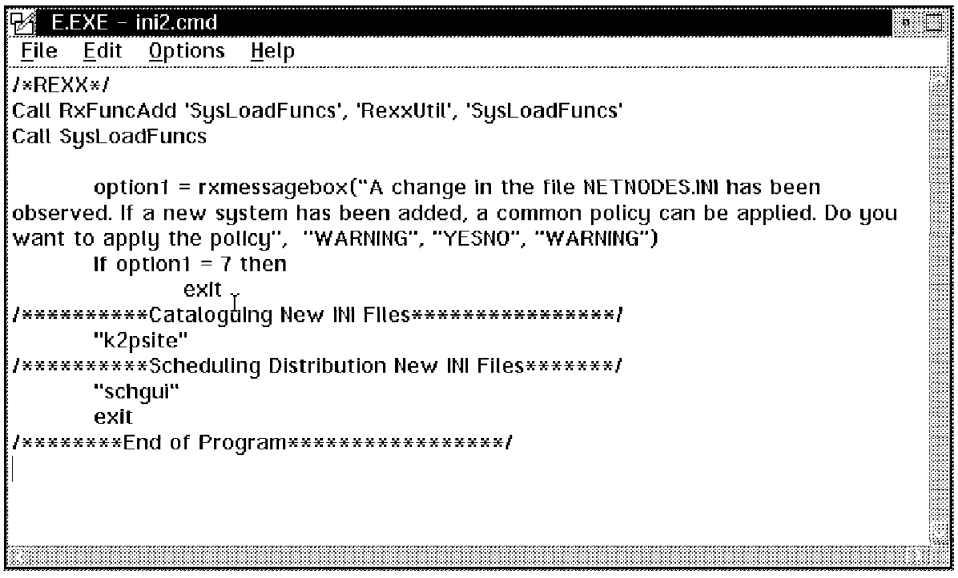


Figure 310. INI2.CMD Program

This program only calls the graphic interfaces for the Software preparation and for the Scheduler. The base component of the scheduler had to be started

already. Normally, when you start SystemView, it starts the base component. You can check the Process Manager to be sure that a program called SCHBASE.EXE is executing.

The first part of the program is the instructions to implement a pop-up window with two options. This application needs to be run under PMREXX.

Chapter 8. Windows 95 Management

This chapter provides an overview of the management features on Windows 95. These features are available on the Windows 95 CD-ROM. After giving an overview of Systems Management in Windows 95, we describe the following:

- The Registry
- The Registry Editor and Registry Keys
- The System Policy Editor and User Profiles
- The System Monitor utility
- The MS SNMP agent

Please be aware that there are many other management functions available that are not covered in this chapter. Refer to the Microsoft Windows 95 Resource Toolkit for detailed information on all management functions in Windows 95.

The toolkit is a book that comes with a CD (ISBN 1-55615-678-2). It is also on the WIN95 CD and is available on the World Wide Web at the following URL:

`http://www.microsoft.com/windows/software/reskit.htm`

8.1 Systems Management Overview in Windows 95

Windows 95 has many built-in functions to allow itself to be managed by other machines. These functions provide limited access to:

- Configuration Management
- Performance Management
- Operations Management (Backup/Disk Management utilities)
- Business Management (Security Management)

Configuration Management is achieved using the Registry, which is a central repository of workstation configuration data.

Performance Management is performed by the System Monitor, a tool that allows a manager to monitor workstation-critical resources such as CPU and memory. The Network Monitor agent complements performance management allowing network monitoring.

Two functions are available for limited **Operations Management**: backup and disk utilities.

Security Management allows a System Administrator to set up system policies and user profiles to customize the workstation environment for different users with specific needs and access authorizations.

8.2 Windows 95 Registry

Microsoft eliminated complexities and limitations of control files such as CONFIG.SYS, AUTOEXEC.BAT and INI files by creating the Registry. The Registry is a hierarchical database that stores workstation configuration data. It places all of the configuration information needed by applications and the operating system in one structured and expandable repository.

Control files still exist under Windows 95 for compatibility matters. CONFIG.SYS, AUTOEXEC.BAT and INI files are kept so that applications that require them will not fail. The operating system still recognizes these control files and the values within them.

Along with configuration information, the Registry stores user profile settings and software class definitions. User profile settings allow Windows 95 to have a particular customization for each user, such as desktop color and icons. Software classes provide information for OLE and for associating filename extensions with applications (this can be roughly compared to OS/2′s object-oriented model).

Although the Registry is one single logical entity, its values are kept in two different files: USER.DAT and SYSTEM.DAT. USER.DAT keeps all user-specific information, while SYSTEM.DAT stores hardware and other configuration information. Both files are kept in the windows SYSTEM directory. However, USER.DAT may also reside on a network drive, allowing user profiles to be accessed from any computer in that network.

Since critical data resides on the Registry, the Registry files become just as critical. For that matter, there are facilities to back up and restore the Registry in case a problem occurs. This is done first automatically by the operating system every time it is started successfully; USER.DAT and SYSTEM.DAT are copied to USER.DA0 and SYSTEM.DA0 respectively. If problems happen on the next boot, you may copy the backup files onto the current files and restore the system to the last successful configuration. The emergency startup diskette contains a utility that allows Registry editing and re-creation. These can also be used when the registry is corrupted.

8.3 The Registry Editor and Registry Keys

Every time any configuration change is carried out on the workstation, the Registry is updated to reflect this change. These modifications may take place when you use Control Panel programs, when you add hardware (Plug-and-Play or not) or during the installation of applications that use the Registry. You may, however, want to view or manually alter values in the Registry. This may be done using the Registry Editor.

Note

The Registry Editor will not warn you of incorrect values entered manually. Always use the options in the Control Panel or the System Policy Editor when possible to avoid making mistakes that could corrupt the Registry and prevent your system from rebooting.

The Registry Editor (REGEDIT.EXE) is automatically installed when you install Windows 95 from a CD-ROM. It is located under the Windows directory. It is also found in the diagnostics window. To start the Registry Editor, use the **Run...** option in the Start menu. Type `regedit`, then press **OK**. The following window will appear:

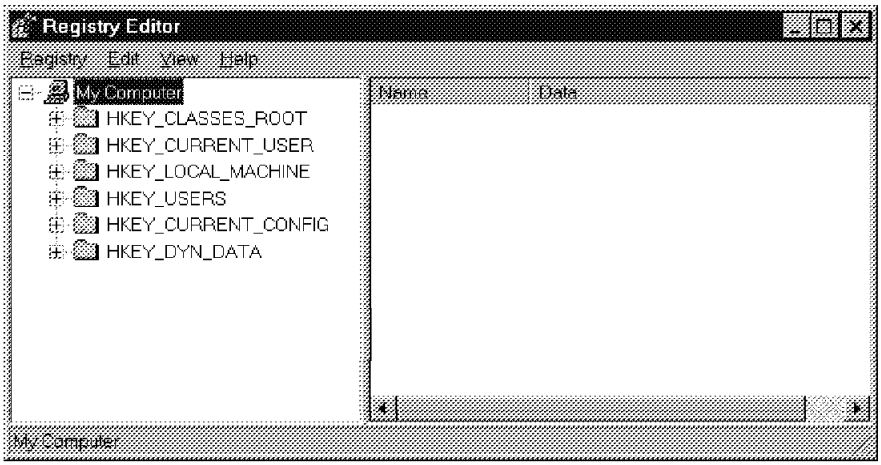


Figure 311. Registry Editor Window

The values in the Registry are stored with keys. Each key contains values (data items) and optionally subkeys. Subkeys may also contain values and subkeys, thus creating a hierarchical tree structure or directory, as shown in Figure 312.

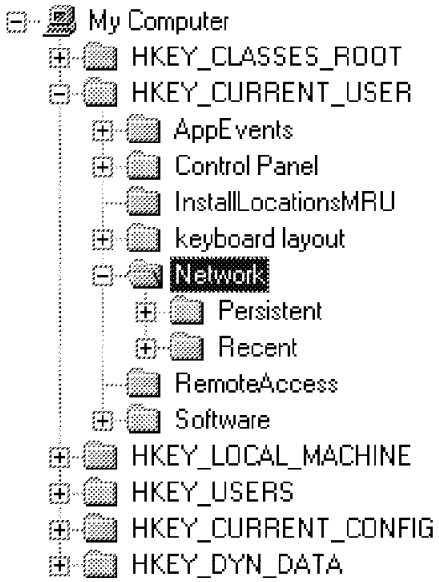


Figure 312. Registry Structure Example

There are six root keys in the Registry:

- Hkey_Local_Machine
- Hkey_Current_Config
- Hkey_Classes_Root
- Hkey_Users
- Hkey_Current_User
- Hkey_Dyn_Data

Hkey_ identifies a unique handle for each key. This handle will be referenced by applications that access Registry values. The values may be either binary or text. They are displayed in the right side of the Registry Editor window, as shown in Figure 311.

Hkey_Local_Machine contains all configuration data for the workstation. It is the source of configuration information based on local applications, the operating system and device drivers on the system. Its main subkeys are:

- Config - this subkey stores different hardware configurations for the same workstation (for example, if the computer is connected to a network, or if a device has been removed). These different configurations are shown in the hardware profile list under the System option in the Control Panel.
- Enum - this subkey stores windows bus enumerators. The operating system assigns an ID to each device on the bus. These IDs are called bus enumerators and are stored under this subkey, together with the device's configuration information such as device type, assigned drive letter and manufacturer.
- Software - this subkey contains information on all software registered with the operating system. Filename extension associations with applications, OLE information, descriptions, version numbers and other important software data are stored here.
- System - under the System\Control subkey, startup parameters for the system are stored. These include the Computer Name, keyboard layouts, identification for the current configuration, and OS device drivers to be loaded at startup.

Network, Hardware and Security information are also kept under Hkey_Local_Machine.

Hkey_Current_Config points to the current configuration being used by the workstation in Hkey_Local_Machine\Config.

Hkey_Dyn_Data is responsible for storing dynamic information directly on RAM. Any information that changes rapidly is stored here (for example, network component statistics and loaded device drivers).

Hkey_Classes_Root refers to software information contained in Hkey_Local_Machine, mainly regarding OLE and shortcuts.

Hkey_Users contains information about all users that logged on to the workstation. User profile information such as Control Panel settings, keyboard layouts, network connections, and software settings (pointing to Hkey_Local_Machine\Software) specific to each user are stored here.

Hkey_Current_User contains the values for the user that is currently logged on to the machine.

Many other subkeys have important values. Please refer to the Microsoft Windows 95 Resource Toolkit for additional information on other Registry values.

8.4 The System Policy Editor and User Profiles

User profiles in Windows 95 allow the operating system to store different system configurations for each user that logs on to the system. This means that in the Windows 95 machine you choose to use in your network, you may always have your own desktop settings automatically available when you log in.

System policies complement user profile functions for the network administrator. They allow you to set a standard profile for all or some of the workstations on the LAN.

The System Policy Editor provided with Windows 95 will assist you in setting up either system policies or individual user profiles. The values in both situations concern Registry keys, and the System Policy Editor will help you to make sure that the correct values are updated in the Registry.

To install the System Policy Editor, double-click on the **Add/Remove Programs** icon in the Control Panel. Choose the **Windows Setup** tab, then click on **Have Disk**. Choose **Browse** and select the path ADMIN\APPTOOLS\POLEDIT in the Windows 95 CD. Click on **OK**, and then click on **OK** again. Highlight the System Policy Editor check box and click on **Install**.

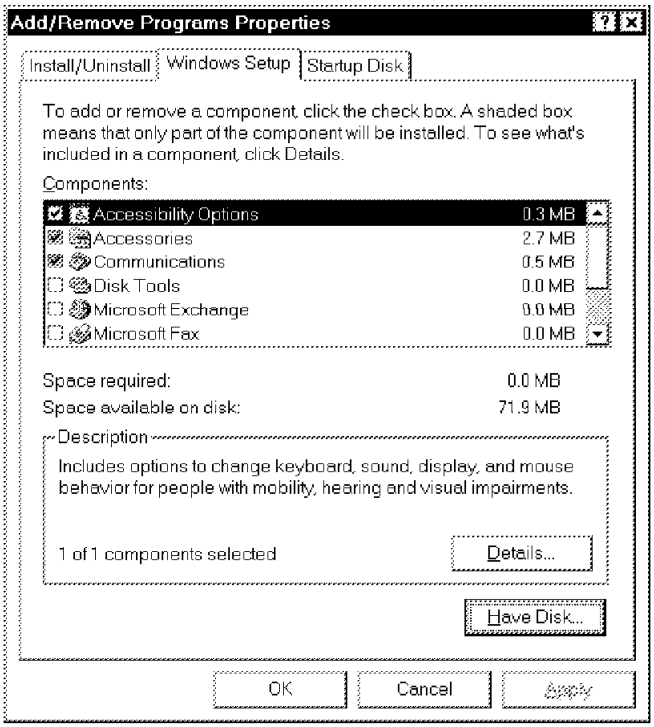


Figure 313. Add/Remove Programs Window, Windows Setup Tab

To run the System Policy Editor, choose **Run...** from the Start menu and type `poledit`, then press **OK**. This will display the System Policy window.

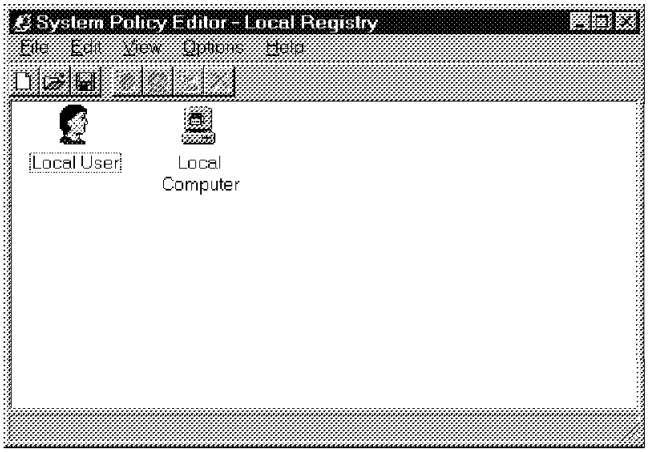


Figure 314. System Policy Editor Window Editing Local Registry

Select **File**, then **Open Registry** to edit Registry values. This will display two icons: one for Local User, and another for Local Computer. Choose the icons according to the values you wish to update. Under the Local User icon you may update user-related configuration values for the Control Panel, the Desktop, the Network, the OS Shell and the System itself. Figure 315 shows you what the Local User configuration looks like.

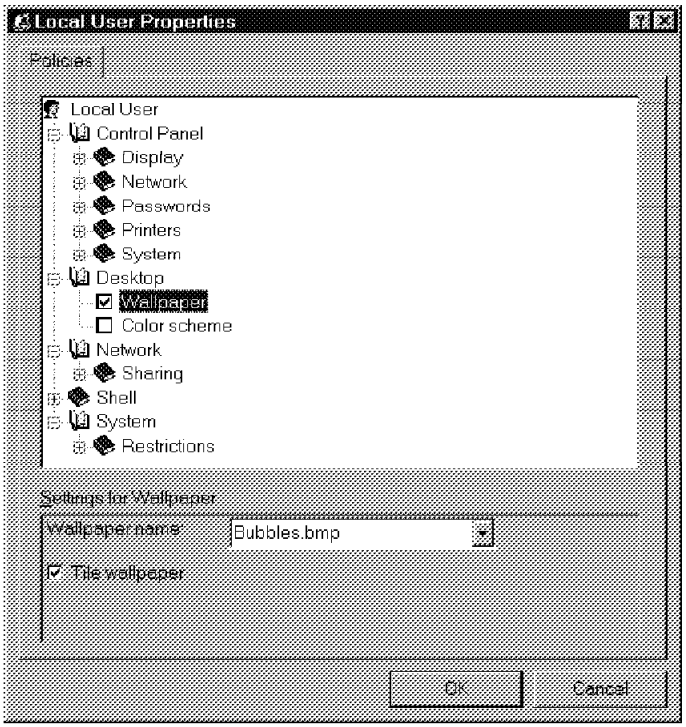


Figure 315. Local User Settings for Wallpaper in the System Policy Editor

Under the Local Computer icon you may customize values for the Network and for the System related to the actual workstation.

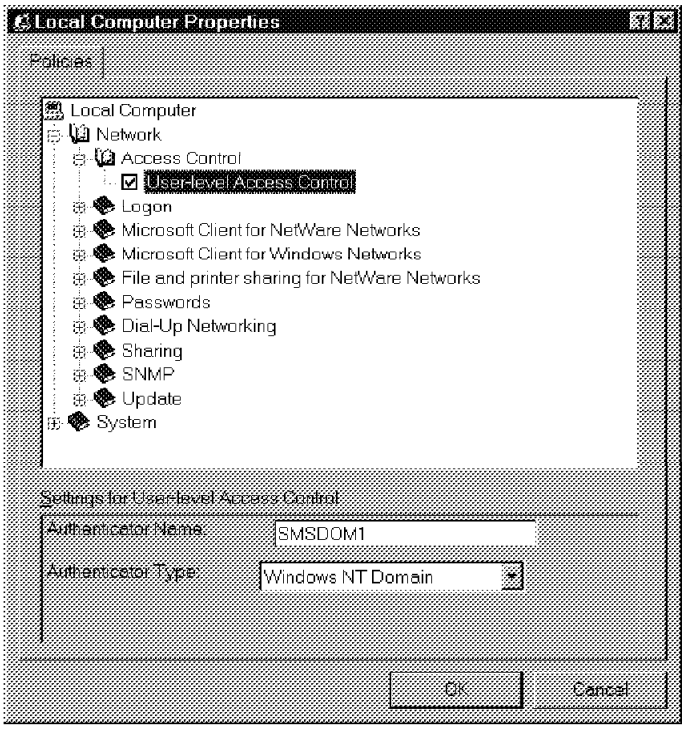


Figure 316. Local Computer Settings for Network User-Level Access Control in the System Policy Editor

Additional information on the System Policy Editor, user profiles and system policies may be found in the Microsoft Windows 95 Resource Toolkit.

8.5 The System Monitor Utility

Windows 95 provides a performance monitoring tool called System Monitor. The System Monitor allows the monitoring of system resources such as memory, CPU utilization and network activity on a local or remote workstation. The performance information is collected in the Registry, and then graphically displayed in the System Monitor window.

To install System Monitor, open the **Add/Remove Programs** icon in the Control Panel. Under the Windows Setup tab, make sure the **Accessories** check box is highlighted. Select it and press **Details**. Select the **System Resource Monitor** and click on its check box. Then press **OK**. After the files are copied, the System Monitor installation is finished. You will have to update the registry to begin data capture, since the default is to not collect data.

Now choose **Run...** from the Start menu. Then type `sysmon` and press **OK**. This will display the System Monitor window.

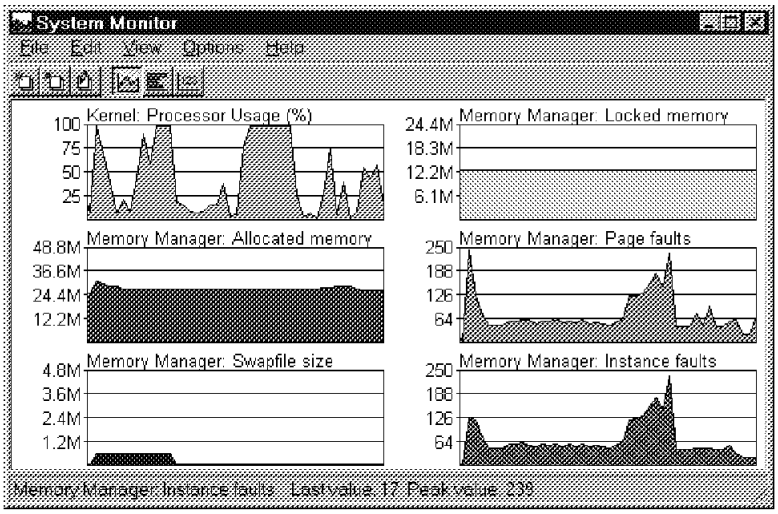


Figure 317. Sample of a Customized System Monitor Window

System Monitor allows you to monitor the following system resources:

- File System
  - Bytes read/second
  - Bytes written/second
  - Dirty data
  - Reads/second
  - Writes/second
- Kernel
  - Processor Usage (%)
  - Threads
  - Virtual Machines
- Memory Manager
  - Allocated memory
  - Discards
  - Disk cache size
  - Free memory
  - Instance faults
  - Locked Memory
  - Maximum disk cache size
  - Minimum disk cache size
  - Page faults
  - Page-ins
  - Page-outs
  - Swapfile defective
  - Swapfile in use
  - Swapfile size
  - Swappable memory
- MS Network Client
  - Bytes read/second
  - Bytes written/second
  - Number of nets
  - Open files
  - Resources
  - Sessions
  - Transactions/second
- MS Network Server

  - Buffers
  - Bytes read/second
  - Bytes written/second
  - Bytes/second
  - Memory
  - Server Network Buffers
  - Server Threads
- Network Monitor Performance Data
  - Adapter broadcasts/second
  - Adapter bytes/second
  - Adapter frames/second
  - Adapter multicasts/second

In the above metrics, the adapter can be Ethernet or token-ring.

System Monitor graphs may be customized to show any of the above values on line, bar or numeric charts. To add or remove monitored values, use the **Add...** or **Remove...** option under the Edit menu.

Since performance values are kept in the Registry, it is possible to add new meters to the System Monitor using drivers that write to the Registry. This is documented in the Microsoft Windows 95 Device Development Kit.

The System Monitor will allow you to see the performance on your system, but will not perform any active monitoring, such as establishing thresholds and generating error notifications.

8.6 The Windows 95 SNMP Agent

An SNMP agent is provided with the Windows 95 CD. It allows the Windows 95 workstation to be managed by an SNMP manager such as NetView for AIX, NetView for OS/2 and NetView for Windows.

To install the Windows 95 SNMP agent, open the **Network** icon in the Control Panel. Click on the **Add...** button, select **Service** and press **Add...**. On the Select Network Service window, select **Have Disk...**. Enter the path name ADMIN\NETTOOLS\SNMP on the Windows 95 CD-ROM and click on **OK**. Select the **Microsoft SNMP Agent** on the Select Network Service window, then press **OK**. If Windows prompts you for additional files, specify the Windows 95 path (usually C:\Windows), or the Windows System path (usually C:\Windows\System). All of the files should be there but the install program won't find them by itself. This is a bug in the level of code that we have.

The SNMP agent will automatically start after the next boot. You will not be able to see it as a task, but you may use the SystemView for OS/2 Process Manager to make sure it is running. Customize the SNMP agent parameters prior to re-starting the workstation.

Use the System Policy Editor (8.4, "The System Policy Editor and User Profiles" on page 194) to customize the SNMP agent. On the System Policy Editor window, choose **File**, then **Open Registry**. Double-click on the **Local Computer** icon. The SNMP settings will be under the Network book, as shown in the following figure:

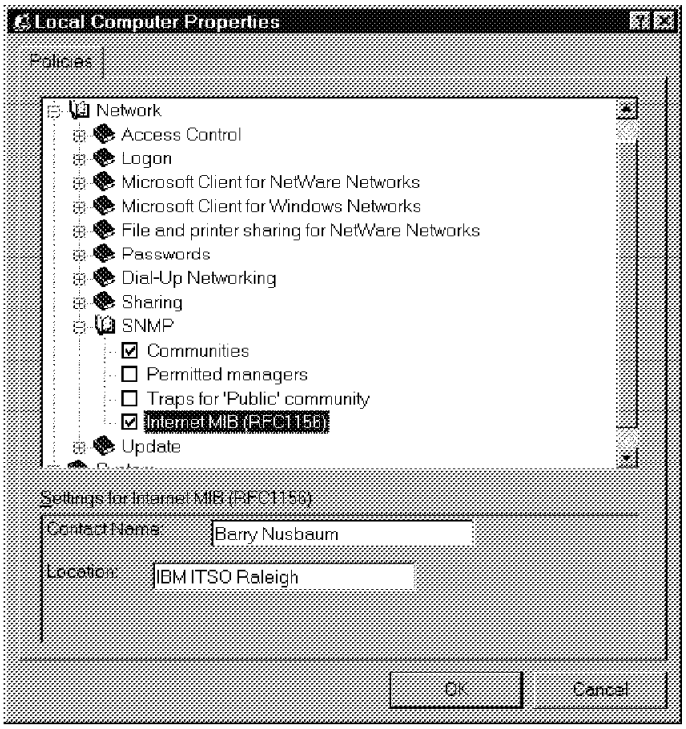


Figure 318. Customizing SNMP Parameters in the System Policy Editor

Customize the agent with the community name, contact name and location. To do that, highlight the check box corresponding to the item you want to customize, and enter the desired values in the Settings field in the bottom of the window. We set the Community value to `public`, but in other enviornments the value would be different to enforce local security standards. Figure 318, for example, shows settings for Contact Name and Location.

After your changes are made, select **OK** and exit the System Policy Editor. You have finished installing and configuring the SNMP agent provided with Windows 95. Now reboot the machine to make the changes valid, and you will be able to request SNMP information from your SNMP manager workstation to this machine. You might wish to use a MIB Browser, or MIB appliation builder from one of the SNMP managers, to monitor specific values.

Chapter 9. Problem Determination Data

This chapter shows you how to automatically gather problem determination data in a managed machine for the following components:

- System Performance Monitor/2 performance data
- TCP/IP trace data file

When the information is gathered, it will automatically be transferred to the SystemView for OS/2 Manager from the managed client.

The process will be started by a SystemView alert signaling that a specific problem has occurred which requires gathering problem determination data from a component. The components, as specified above, are TCP/IP, SPM/2 and Theseus/2.

9.1 System Performance Monitor/2 Performance Data

SPM/2 is a tool used to assist in analyzing the performance of workstations running OS/2. It works with Theseus/2, a memory analysis program, to provide real-time and historical data for performance analysis and tracking. It is also possible to track the performance of remote systems using the SPM/2 distributed feature (client) on machines with peer services. We used the peer services associated with OS/2 LAN Server 4.0 and also associated with OS/2 Warp Server. There are several CSDs on LAN Server 3.0 that are necessary for peer services to work correctly for SPM/2. Thus, we chose to only use LAN Server 4.0′s peer services. If you are not starting peer services automatically, you can start it with the net start peer command.

SPM/2 functions may be performed through the graphical user interface (GUI) as well as through the command line. In this scenario, we set up our environment using the GUI, and use the command line to perform the automated functions.

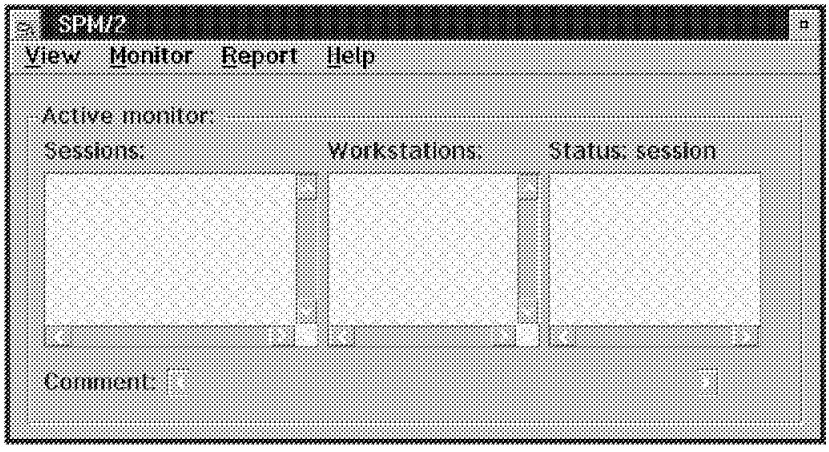


Figure 319. SPM/2 Graphical User Interface

Our scenario consists of SystemView monitoring CPU activity. When SystemView detects a busy CPU condition (100% utilization) for over 5 minutes, it triggers our automated process. Our process starts SPM/2 to collect CPU performance data

by process/application for 5 minutes. After 5 minutes, we stop the data collection and generate a report on CPU usage. As a last step, our process analyzes the report and informs the SystemView Manager of the top 5 CPU users (processes or applications) by sending genalerts. We first show SPM/2 customization, and then go over the necessary SystemView customization steps.

To track resource performance with SPM/2, you must define *monitors*. To define a monitor for the CPU utilization, open the Monitor setup menu on the SPM/2 GUI (Figure 319 on page 201) and choose **Setup**, then **New**. Enter a comment in the *Comment* field for the description of your monitor. For example, type the following:

```
CPU Monitor by process
```

If no workstations appear in the Available window, select the **Query** button so SPM/2 can do a NetBIOS broadcast to find workstations that have SPM/2 installed and available for reporting. Double-click on your workstation to add it to the selected workstations list.

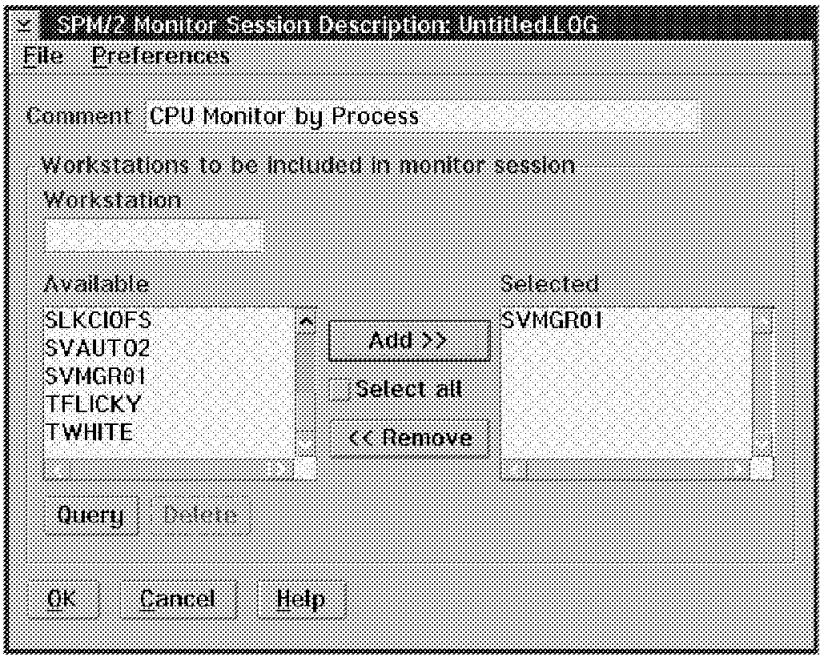


Figure 320. SPM/2 Monitor Session Description Window

Now choose **Resources** under the Preferences pull-down menu to define CPU as the monitored resource. The following window will appear:

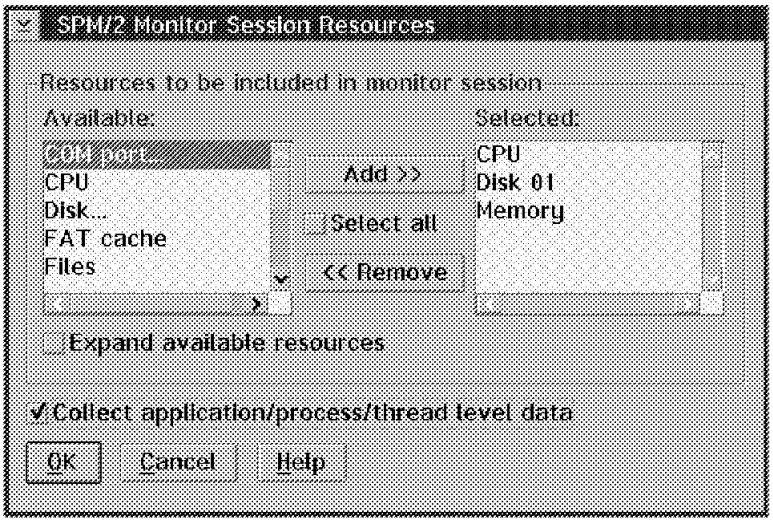


Figure 321. SPM/2 Monitor Session Resources

The above window shows the available resources for SPM/2 to monitor on the left side, and the default selected resources on the right side. Remove all resources, except CPU, from the Selected resource window on the right side by double-clicking on them. Highlight the **Collect application/process/thread level data** check box to make SPM/2 gather detailed data. Select **OK** twice. Make sure that you save your monitor on a disk with plenty of space. Your monitor will be saved in a .LOG file, which will also contain the performance data collected. We saved our monitor data in CPUMON.LOG.

Now set up the report to analyze data collected by CPUMON.LOG. To set up a report, open the Report pull-down menu on the SPM/2 GUI (Figure 319 on page 201) and choose **Setup**, then **New**. Type the title of your report in the Title field. The title of our example is *Top 5 CPU intensive processes*. The available monitors are shown below in the left side box. Double-click on **CPUMON.LOG** to add it to the selected monitors list.

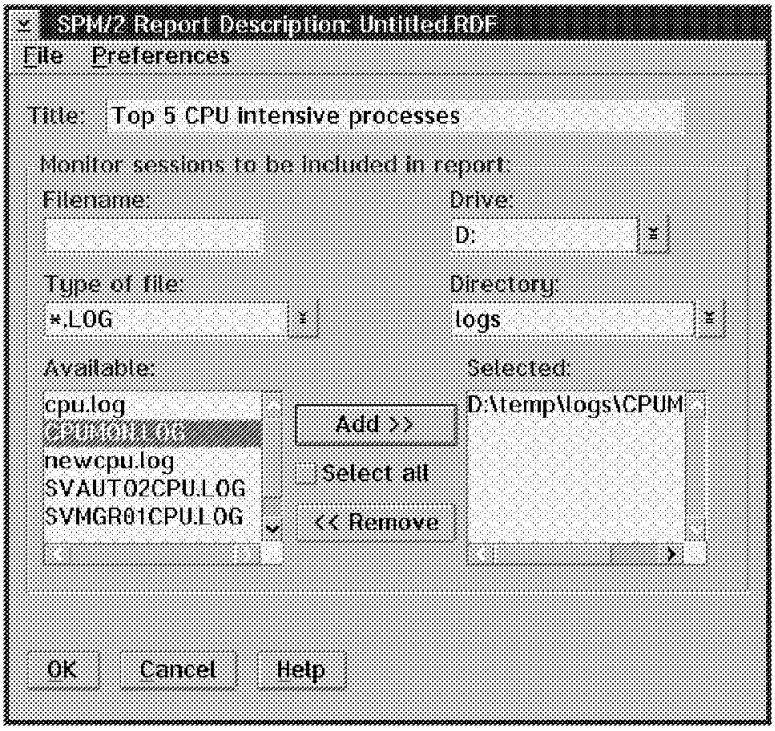


Figure 322. SPM/2 Report Description Window

SPM/2 can generate three types of reports: tabular, summary, and dump reports. The format that best suited our scenario was the summary. To select a summary report type, choose the **Format** option under the Preferences pull-down menu. Make sure the **summary** option is checked. After the **summary** option is checked under the Format option, we can use the **Summarization Level** option under the Preferences pull-down menu to get the details from our summary report. Choose the Preferences pull-down menu, **Summarization Level**, then **Process...**. This will bring you to the following window:

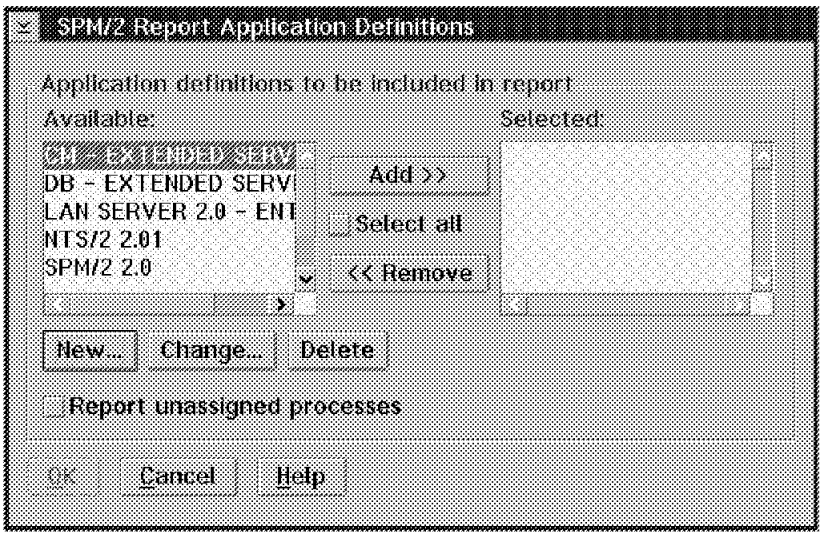


Figure 323. SPM/2 Report Application Definitions

This window allows you to associate executable files with applications. For example, we know that ADSM/2 has the following executable files installed:

DSM.EXE, DSMC.EXE, DSMADM.EXE and DSMADMC.EXE. Using the SPM/2 Report Application Definitions window, we can associate these executables with the ADSM/2 application and have our report show a total for ADSM/2 instead of only listing each separate executable. This saves time since we do not have to always remember which program belongs to which application.

You may use the already defined applications or define new ones to suit your environment. Use the **New...** button to define new applications. To choose which applications will be included in the report, double-click on them in the Available box (found on the left side in Figure 322 on page 204). The applications in the Selected box will be considered for the report.

Check the **Report unassigned processes** check box to have processes that do not belong to any defined application reported on as well. Now select **OK** twice and save your report. Reports are saved with the .RDF extension. We named our report CPUMON.RDF.

We are now ready to collect data and generate reports. This could be done using the graphical interface, but since we are focusing on automation, we will use the command line instead. The following REXX procedure will provide our automated gathering/reporting/analyzing process:

```
/* REXX for OS/2                                                  */
/*                                                                */
/* This programs starts SPM to collect performance data for       */
/* five minutes. After that, sorts the output and determines      */
/* what are the top 5 CPU consumers, issuing genalerts for        */
/* each one.                                                      */

Trace off
Call RxFuncAdd "SysLoadFuncs","RexxUtil","SysLoadFuncs"
Call SysLoadFuncs

LogFile = 'D:\TEMP\LOGS\CPUMON.LOG'
Report  = 'D:\TEMP\LOGS\CPUMON.RDF'
Output  = 'D:\TEMP\LOGS\CPUMON.SUM'
Sorted  = 'D:\TEMP\LOGS\CPUMON.SRT'
String  = '--------  --------  ----------->'

'C:\SPM2V2\SPMISTRT ' LogFile                    /* Start data collection   */
 RC = SysSleep(300)                              /* Wait five minutes       */
'C:\SPM2V2\SPMISTOP /DRAIN ' LogFile             /* Normal stop             */
'C:\SPM2V2\SPMRDF ' Report                       /* Generate Summary Report */
'SORT /R /+12 < 'Output' > 'Sorted               /* Sort from column 12 on  */
 RC = SysFileSearch(String,Sorted,Lines)         /* Get only useful lines   */
                                                 /*                         */
 i=1                                             /* Generate alert for the  */
 do 5                                            /* first five processes    */
    ProcessName = Word(Lines.i,8)                /*                         */
  'GENALERT /T:"Number '||i||' CPU user: '||,     /*                         */
             ProcessName||'"',                   /*                         */
            '/APP:SPM ',                         /*                         */
            '/SEV:0 ',                           /*                         */
            '/TYPE:APPWRN '                      /*                         */
 /* RC = SysSleep(2)                                Uncomment if necessary  */
    i  = i + 1                                   /*                         */
 end                                             /*                         */
                                                 /*                         */
 Exit                                            /* The End                 */
```

Figure 324. PERF.CMD Sample REXX Procedure

Remember to substitute all path and filename references to the path and file names used in your environment.

As a reference, the summary report generated by SPM/2 would look like the following figure:

```
 Report Type     :  PROCESS  ( SUMMARY )                                                                    Report Date:  02-28-96
        Title    :  Top 5 CPU intensive processes                                                                Time:  12:10:31
        Filename :  D:\TEMP\LOGS\CPUMON.RDF

 Monitor Session :  D:\temp\logs\CPUMON.LOG ( CPU Monitor by Process )

 Start Date/Time :  02-28-96  12:09:36      *** Defaulted to actual collection start time.
 Stop  Date/Time :  02-28-96  12:10:13      *** Defaulted to actual collection stop time.

    Sum Interval :  00:00:36                *** Defaulted to actual collection period.

*************************************************************************************************************************************************

 Workstation     :  SVMGR01

          CPU

          ----- Processor ------  ------- Threads ------  ---------- Interrupts ----------
 Summary                 Busy                  Avg                          Service
  Time      % Util        Time     Dispatch   Timeslice     % Util     Rate       Time          Application   Program   PID
========  ========  ============  ========  ============  ========  ========  ============  ============  ========  =====
12:10:13   100.00   00:00:10.055    2143    00:00:00.005     6.01      164    00:00:00.604

             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>  CM - EXTENDED

             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                ACS3EINI  051

             0.09   00:00:00.009      11    00:00:00.001  --------  --------  ------------>  LAN SERVER 2.

             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                LSDAEMON  017
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                MSRV      053
             0.07   00:00:00.007       8    00:00:00.001  --------  --------  ------------>                WKSTA     041

             0.00   00:00:00.000       1    00:00:00.000  --------  --------  ------------>  NTS/2 2.01

             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                LANMSGEX  007
             0.00   00:00:00.000       1    00:00:00.000  --------  --------  ------------>                LANDLL    023

             0.18   00:00:00.018       4    00:00:00.004  --------  --------  ------------>  SPM/2 2.0

             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                NBQRSPND  054
             0.17   00:00:00.017       2    00:00:00.009  --------  --------  ------------>                SPMDCF    263
             0.01   00:00:00.001       2    00:00:00.000  --------  --------  ------------>                SPMILOG   262
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                SPMNBL    024
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                SPMNET    028
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                SPMSNAPL  027

            33.37   00:00:05.366     458    00:00:00.012  --------  --------  ------------>  SYSTEMVIEW

             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                ALERTMGR  089
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                EQNKCTKB  005
             1.26   00:00:00.127     224    00:00:00.001  --------  --------  ------------>                EQNRCKB   003
            31.82   00:00:05.210     216    00:00:00.024  --------  --------  ------------>                MONBASE   068
             0.29   00:00:00.029      18    00:00:00.002  --------  --------  ------------>                NETFBASE  060
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                SCHBASE   087
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                SHRBASE   075

             0.00   00:00:00.000       3    00:00:00.000  --------  --------  ------------>  TCP/IP

             0.00   00:00:00.000       1    00:00:00.000  --------  --------  ------------>                INETD     079
             0.00   00:00:00.000       1    00:00:00.000  --------  --------  ------------>                SNMPD     093
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                VDOSCTL   021

            46.11   00:00:04.635    1666    00:00:00.003  --------  --------  ------------>  -unassigned-

             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                REMMAIN   043
             0.01   00:00:00.001       2    00:00:00.000  --------  --------  ------------>                NETMSG    059
             0.51   00:00:00.052     282    00:00:00.000  --------  --------  ------------>                CNTRL     008
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                MUGLRQST  050
             0.01   00:00:00.001       5    00:00:00.000  --------  --------  ------------>                DDAEMON   029
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                SPDAEMON  030
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                CMD       245
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                EPWDDR3   022
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                EPWROUT   020
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                PMSPOOL   035
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                HARDERR   026
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                LOGDAEM   018
            42.28   00:00:04.251     952    00:00:00.004  --------  --------  ------------>                IBMAV2    260
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                IBMAVSD   096
             0.00   00:00:00.000       0    00:00:00.000  --------  --------  ------------>                sysinit   001
```

Figure 325. SPM/2 Summary Report

Note on Running SPM/2 and SystemView

You may notice the 100% CPU usage in Figure 325 as well as high CPU usage for the SystemView tasks (specifically MONBASE).

MONBASE is responsible for monitoring the system according to what is set from the System Monitor GUI. To measure CPU utilization, MONBASE starts a low priority looping thread in the background. Other performance tools (such as SPM/2) include this looping thread in their measurement, resulting in utilization always equal to 100%.

This may be avoided if you stop SystemView or if you prevent MONBASE from monitoring CPU utilization when measuring performance with SPM/2. This can be achieved in the following ways:

- If you choose to stop SystemView:

  Issue the NETFBASE SHUTDOWN command in an OS/2 window.

- If you choose to stop CPU monitoring by SystemView:

  Rename the file MONCPU.DLL when NETFBASE is not running. This will prevent SystemView from monitoring CPU utilization.

SystemView must be customized to:

- Monitor CPU utilization, issuing an alert for CPU usage of 100% for over 5 minutes
- Start the PERF.CMD program when the above alert is received
- Forward PERF.CMD genalerts to the SystemView Manager

9.2 TCP/IP Trace Data

There are many utilities in TCP/IP that can be used for problem determination. In our scenario, we will collect information provided by:

- Configuration files (SETUP.CMD, MPTN*.INI)
- netstat
- tracerte
- iptrace

These sources of information are described briefly in the following sections. Please refer to your TCP/IP documentation if you need details on these utilities.

9.2.1 TCP/IP Configuration Files

The SETUP.CMD file contains all information on the TCP/IP startup parameters for the workstation, such as adapter and routing configuration. A sample SETUP.CMD could look as follows:

```
route -fh
arp -f
ifconfig lan0 9.24.104.222 netmask 255.255.255.0
REM ifconfig lan1
REM ifconfig lan2
REM ifconfig lan3
REM ifconfig lan4
REM ifconfig lan5
REM ifconfig lan6
REM ifconfig lan7
REM ifconfig sl0
route add default 9.24.104.1 1
route add net 9 9.24.104.1 1
ipgate off
```

Figure 326. Sample SETUP.CMD File

The MPTN\ETC directory holds INI files that keep parameters for TCP/IP and its utilities. Our machine has the following INI files:

```
INI file name     Application
----------------- ------------------------
EXPLORE.INI       Web Explorer
GOPHER.INI        Gopher
NR2.INI           News Reader
PMX.INI           X-Windows
SNMP.INI          SNMP
TCPIP.INI         TCPIP
TCPOS2.INI        Internet Dialer
TELNETPM.INI      Telnet
```

These files together with the SETUP.CMD are useful for problem determination and will be part of the ″package″ we will make available to the Manager.

9.2.2 Netstat

The Netstat command provides TCP/IP information and status for the IP address, routing tables, connections, interface characteristics. We will issue the netstat command with all parameters:

```
netstat -camusprint
```

Our command returned the following values:

```
mbufs obtained from page pool 1408
free mbufs 1330
data mbufs 1
header mbufs 21
socket structure mbufs 21
socket name mbufs 0
socket option mbufs 0
protocol control block mbufs 31
routing table mbufs 3
fragment reassembly mbufs 0
clusters obtained from page pool 56
free clusters 56
times failed to find space 0
times waited for space 0
total number of datagrams received 33358
total number of datagrams sent 17333
datagrams for which no port was found 44
number of drops 0
number of bad chksums 0
number of packets with bad length 0
connections initiated              257
connections accepted               84
connections established            306
connections dropped                0
embryonic connections dropped      35
conn. closed (includes drops)      343
segs where we tried to get rtt     6659
times we succeeded                 6546
delayed acks sent                  2499
conn. dropped in rxmt timeout      0
retransmit timeouts                166
persist timeouts                   0
keepalive timeouts                 216
keepalive probes sent              0
connections dropped in keepalive   32
total packets sent                 16772
data packets sent                  9564
data bytes sent                    5299260
data packets retransmitted         18
data bytes retransmitted           22505
ack-only packets sent              5659
window probes sent                 0
packets sent with URG only         0
window update-only packets sent    836
control (SYN|FIN|RST) packets sent695
RST packets sent                   0
total packets received             17968
packets received in sequence       11270
bytes received in sequence         7095213
packets received with ccksum errs  0
packets received with bad offset   0
packets received too short         0
duplicate-only packets received    30
duplicate-only bytes received      9283
packets with some duplicate data   12
dup. bytes in part-dup. packets    2800
out-of-order packets received      2595
out-of-order bytes received        96813
packets with data after window     6
bytes rcvd after window            6
packets rcvd after close           2
rcvd window probe packets          6
rcvd duplicate acks                217
rcvd acks for unsent data          0
rcvd ack packets                   7338
bytes acked by rcvd acks           5299572
rcvd window update packets         85
total packets received 57963
checksum bad 0
packet too short 0
not enough data 0
ip header length < data size 0
ip length < ip header length 0
fragments received 449
frags dropped (dups, out of space) 0
fragments timed out 3
packets forwarded 0
packets rcvd for unreachable dest 2
packets forwarded on same net 0
requests for transmission 39923
output packets discarded because no route could be found 0
input packets delivered successfully to user-protocols 57090
```

Figure 327 (Part 1 of 3). Netstat Command Output

```
input packets with an unknown protocol 449
output packets successfully fragmented 0
output fragments created 0
fragmentation failed 0
successfully assembled packets 223
-------------------------------------------------------------------------------
                          AF_INET Address Family :

SOCK     TYPE     FOREIGN PORT     LOCAL PORT     FOREIGN HOST     STATE
====  =========  =============   =============   =============  =============
697      DGRAM              0            1209         0.0.0.0    UDP
694      DGRAM              0            1208         0.0.0.0    UDP
691      DGRAM              0            1207         0.0.0.0    UDP
688      DGRAM              0            1206         0.0.0.0    UDP
685      DGRAM              0            1205         0.0.0.0    UDP
615      DGRAM              0            1170         0.0.0.0    UDP
611      DGRAM              0           13991         0.0.0.0    UDP
610      DGRAM              0               0         0.0.0.0    UDP
140     STREAM     telnet..23            1046    9.24.104.124    ESTABLISHED
120     STREAM              0            6000         0.0.0.0    LISTEN
36      STREAM              0            1024         0.0.0.0    LISTEN
35       DGRAM              0       snmp..161         0.0.0.0    UDP
32      STREAM              0 netviewdm1..729         0.0.0.0    LISTEN
31      STREAM              0        smtp..25         0.0.0.0    LISTEN
27      STREAM              0     sunrpc..111         0.0.0.0    LISTEN
26       DGRAM              0     sunrpc..111         0.0.0.0    UDP
24      STREAM              0        cmd..514         0.0.0.0    LISTEN
23      STREAM              0       exec..512         0.0.0.0    LISTEN
22      STREAM              0         ftp..21         0.0.0.0    LISTEN
21      STREAM              0      telnet..23         0.0.0.0    LISTEN
-------------------------------------------------------------------------------
                          AF_OS2  Address Family :


    destination         router    refcnt        use flags     snmp  intrf
                                                              metric
        9.0.0.0      9.24.104.1       0        5631    U       -1   lan0
        default      9.24.104.1       0           0    U       -1   lan0
     9.24.104.0    9.24.104.222       9       34267    U       -1   lan0
ICMP statistics
packets received 6180
received destination unreachable msgs 417
received time exceeded msgs 0
received parameter problem msgs 0
received source quench msgs 0
received redirect msgs 0
received echo requests 5763
received echo replies 0
received time stamp requests 0
received time stamp replies 0
received address mask requests 0
received address mask replies 0
packets sent 5810
sent destination unreachable msgs 44
sent time exceededed msgs 0
sent parameter problem msgs 0
sent source quench msgs 0
sent redirect msgs 0
sent echo requests 3
sent echo replies  5763
sent time stamp requests 0
sent time stamp replies 0
sent address mask requests 0
sent address mask replies 0
Interface 0: 802.5
physical address    400052005137      MTU 1500

speed 4000000 bits/sec
unicast packets received 39927
broadcast packets received 347071
total bytes received 32178316
unicast packets sent 39776
broadcast packets sent 1197
total bytes sent 9030403
packets discarded on transmission 53
packets discarded on reception 126
received packets in error 0
errors trying to send 0
packets received in unsupported protocols 0
addr       9.24.104.222 interface 0 mask fffffF00 broadcast       9.24.104.255
```

Figure 327 (Part 2 of 3). Netstat Command Output

```
          ARP table contents:

interface     hardware address         IP address   minutes since
                                                      last use
    0          10005aa8d769           9.24.104.108     3
    0          10005a21a05d                0.0.0.0     14
    0          10005ac95035           9.24.104.241     0
    0          400052005143           9.24.104.100     7
    0          10005ab1c42c           9.24.104.209     0
    0          10005ab187f8            9.24.104.30     0
    0          08005a57a0d3            9.24.104.87     0
    0          10005ac92ceb            9.24.104.60     0
    0          400052005150           9.24.104.223     2
    0          10005ab1afe9           9.24.104.109     0
    0          10005ab155da            9.24.104.25     0
    0          400052005152           9.24.104.101     7
    0          10005ab1d731           9.24.104.215     0
    0          10005aa87023            9.24.104.28     0
    0          400052005011             9.24.104.1     0
    0          10005aa8b5ea           9.24.104.191     0
    0          10005ab1b0fe            9.24.104.12     0
    0          10005ab195ad            9.24.104.23     0
    0          10005ab1ac7d            9.24.104.15     0
    0          10005a4f58ce            9.24.104.26     0
    0          10005ab14fcb           9.24.104.124     0
    0          10005a207ca5            9.24.104.86     6
```

Figure 327 (Part 3 of 3). Netstat Command Output

This output will be sent to the SystemView manager together with the other problem determination data.

9.2.3 Traceroute

The traceroute command allows you to see the route that an IP packet follows between your workstation and another. This is sample output for the tracerte 9.32.1.41 command:

```
traceroute to 9.32.1.41 (9.32.1.41), 30 hops max, 38 byte packets
 0  6611ral (9.24.104.1)  0 ms  0 ms  0 ms
 1  6611ral (9.24.104.1)  0 ms  0 ms  0 ms
 2  6611ral.superlab.css.ibm.com (9.24.96.1)  31 ms  0 ms  0 ms
 3  6611slk.sl.dfw.ibm.com (9.24.1.1)  32 ms  62 ms  32 ms
 4  * * *
 5  9.32.108.1 (9.32.108.1)  94 ms  62 ms  156 ms
 6  9.32.1.41 (9.32.1.41)  125 ms *  94 ms
```

Figure 328. Sample tracerte Output

9.2.4 Iptrace

The iptrace tool traces all IP packets received from and sent to an interface. Iptrace creates a dump file called IPTRACE.DMP, which may get formatted by the ipformat tool so that it can be analyzed. We could either send the IPTRACE.DMP file or the formatted output to the manager. Since the dump file is smaller, it is wiser, from a network point of view, to send the dump and have it formatted by the manager.

Iptrace is started by the iptrace command, and must be interrupted by pressing CTRL+C or CTRL+BREAK. In our automated process, we will use a tool to stop iptrace without human intervention. You should write your own routine for that purpose.

Ipformat takes the information in iptrace.dmp, formats it and displays it in a window. You may also redirect the output to a file. The ipformat output looks as follows:

```
 Reading input file....  Please wait

------------------------------- #:1 -------------------------------
  Delta Time:  0.000   Packet Length: 58 bytes (3A hex)
 802.5:  Dest: FF:FF:FF:FF:FF:FF   Source:
90:00:5A:A8:B5:EA
------------------------- ARP --------------------------
 ARP:  Hardware Type:6     (IEEE 802)
 ARP:  Protocol Type:0800 (IP Address)
 ARP:  Hardware Len:6
 ARP:  Protocol Len:4
 ARP:  Operation:1   (ARP Request)
 ARP:  Sender HW address: 10005AA8B5EA
 ARP:  Sender PA: 009.024.104.191.
 ARP:  Target HW address: 000000000000
 ARP:  Target PA: 009.024.104.089.

------------------------------- #:2 -------------------------------
  Delta Time:  0.094   Packet Length: 58 bytes (3A hex)
 802.5:  Dest: FF:FF:FF:FF:FF:FF   Source:
90:00:5A:B1:4F:CB
------------------------- ARP --------------------------
 ARP:  Hardware Type:6     (IEEE 802)
 ARP:  Protocol Type:0800 (IP Address)
 ARP:  Hardware Len:6
 ARP:  Protocol Len:4
 ARP:  Operation:1   (ARP Request)
 ARP:  Sender HW address: 10005AB14FCB
 ARP:  Sender PA: 009.024.104.124.
 ARP:  Target HW address: 000000000000
 ARP:  Target PA: 009.024.104.214.

------------------------------- #:3 -------------------------------
  Delta Time:  0.406   Packet Length: 58 bytes (3A hex)
 802.5:  Dest: FF:FF:FF:FF:FF:FF   Source:
90:00:5A:C9:50:35
------------------------- ARP --------------------------
 ARP:  Hardware Type:6     (IEEE 802)
 ARP:  Protocol Type:0800 (IP Address)
 ARP:  Hardware Len:6
 ARP:  Protocol Len:4
 ARP:  Operation:1   (ARP Request)
 ARP:  Sender HW address: 10005AC95035
 ARP:  Sender PA: 009.024.104.241.
 ARP:  Target HW address: 000000000000
 ARP:  Target PA: 009.024.104.228.

------------------------------- #:4 -------------------------------
  Delta Time:  0.000   Packet Length: 58 bytes (3A hex)
 802.5:  Dest: FF:FF:FF:FF:FF:FF   Source:
90:00:5A:C9:50:35
------------------------- ARP --------------------------
 ARP:  Hardware Type:6     (IEEE 802)
 ARP:  Protocol Type:0800 (IP Address)
 ARP:  Hardware Len:6
 ARP:  Protocol Len:4
 ARP:  Operation:1   (ARP Request)
 ARP:  Sender HW address: 10005AC95035
 ARP:  Sender PA: 009.024.104.241.
 ARP:  Target HW address: 000000000000
 ARP:  Target PA: 009.024.104.180.

------------------------------- #:5 -------------------------------
  Delta Time:  0.000   Packet Length: 58 bytes (3A hex)
 802.5:  Dest: FF:FF:FF:FF:FF:FF   Source:
90:00:5A:C9:50:35
------------------------- ARP --------------------------
 ARP:  Hardware Type:6     (IEEE 802)
 ARP:  Protocol Type:0800 (IP Address)
 ARP:  Hardware Len:6
 ARP:  Protocol Len:4
 ARP:  Operation:1   (ARP Request)
 ARP:  Sender HW address: 10005AC95035
 ARP:  Sender PA: 009.024.104.241.
 ARP:  Target HW address: 000000000000
 ARP:  Target PA: 009.024.104.137.
```

Figure 329. Iptrace Formatted Output

If you are looking for intermittent problems, you can set up the scheduler function to automatically send specific files back to the SystemView for OS/2 manager every day. You can use the Monitor service to set TCP/IP thresholds, and when they are exceeded you can put the reports into a file.

In addition, you can set up a threshold and if the system exceeds the threshold, it can execute a command to capture the data on its own system; it then sends a genalert back to the manager to make the manager aware that the capturing of data has completed. When this alert arrives at the manager, an automated action can take place to transfer the file over the network for further analysis.

Appendix A. Installation of the ServerGuard Adapter

When you want to install the ServerGuard Adapter on a machine that has SystemView for OS/2 installed, you will need two additional pieces of software:

- The ServerGuard support for NetFinity V3.0

  The file is named OEP128A.DSK. You can get the file from *http://www.pcco.ibm.com/files.html* on the Internet. You have to select the files for NetFinity and download OEP128A.DSK to your PC.

  You can create a diskette image from the file that was downloaded. This image contains the modified NetFinity support for the ServerGuard adapter.

- The NETFINST.EXE from the NetFinity 3.0 original product

  The software installed by SystemView for OS/2 and the NetFinity installation method are *not* similar. To install the ServerGuard extension for NetFinity, you must copy the NetFinity installer NETFINST.EXE from the first OS/2 product installation diskette to the SYSVIEW2-BIN subdirectory of your SystemView for OS/2 installation.

After taking care of these prerequisites, you can simply install the ServerGuard-Extension for NetFinity on your SystemView for OS/2 system:

- Click on the **Diskette symbol** on your Warp Connect launch panel.

  The directory for the ServerGuard for NetFinity Installation diskette should appear:

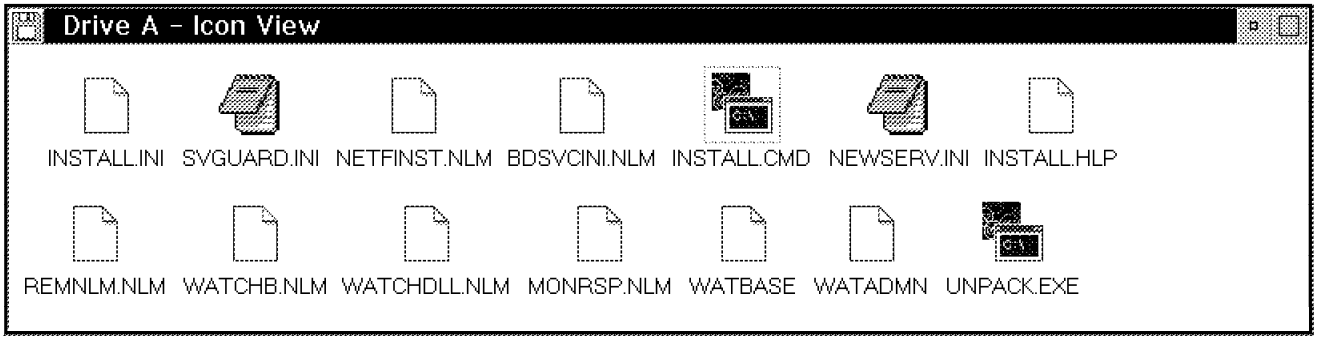


Figure 330. ServerGuard for NetFinity Installation Diskette

- Click on **INSTALL.CMD**.

  The pop-up window NetFinity Install (Part 1) appears.

  Change the “Directory to install to” to the directory where your SystemView for OS/2 is installed (usually `C:\SYSVIEW\BIN`).

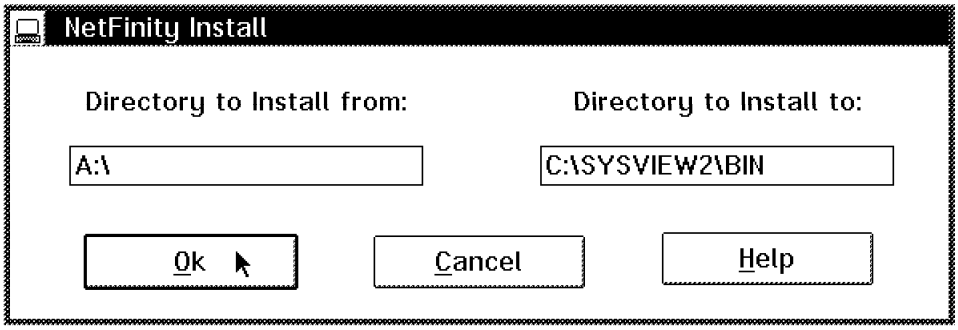


Figure 331. NetFinity Install (Part 1)

- Click on **OK**.

  Next, the pop-up window NetFinity Install (Part 2) appears.

  The entry fields “Directory to Install from ” and “Directory to Install to” have already been filled by the previous dialog and are greyed out now.

  You can choose one of three installation options using the radio buttons provided:

  1. *ServerGuard Installation - Client*

     Using this option, you only install the base components of the NetFinity support for the ServerGuard adapter.

     This choice is the correct choice if you only want to manage the ServerGuard Adapter remotely. You normally do this if the server is located in a separate room and if it is dedicated to the server function.

  2. *ServerGuard Installation - Manager*

     Using this choice, you only install the GUI components of the NetFinity support for the ServerGuard adapter.

     This choice is the correct choice for the SystemView for OS/2 managing machine.

  3. *ServerGuard Installation - Local Management*

     Using this choice, you install the base and GUI components of the NetFinity support for the ServerGuard adapter.

     This choice is the correct choice if you want to manage the ServerGuard Adapter locally.

     ServerGuard Local Management

     Because you have the GUI component for the ServerGuard adapter extension installed, you are also able to manage remote ServerGuard adapters from this workstation.

  The NetFinity Installation pop-up window looks as follows:

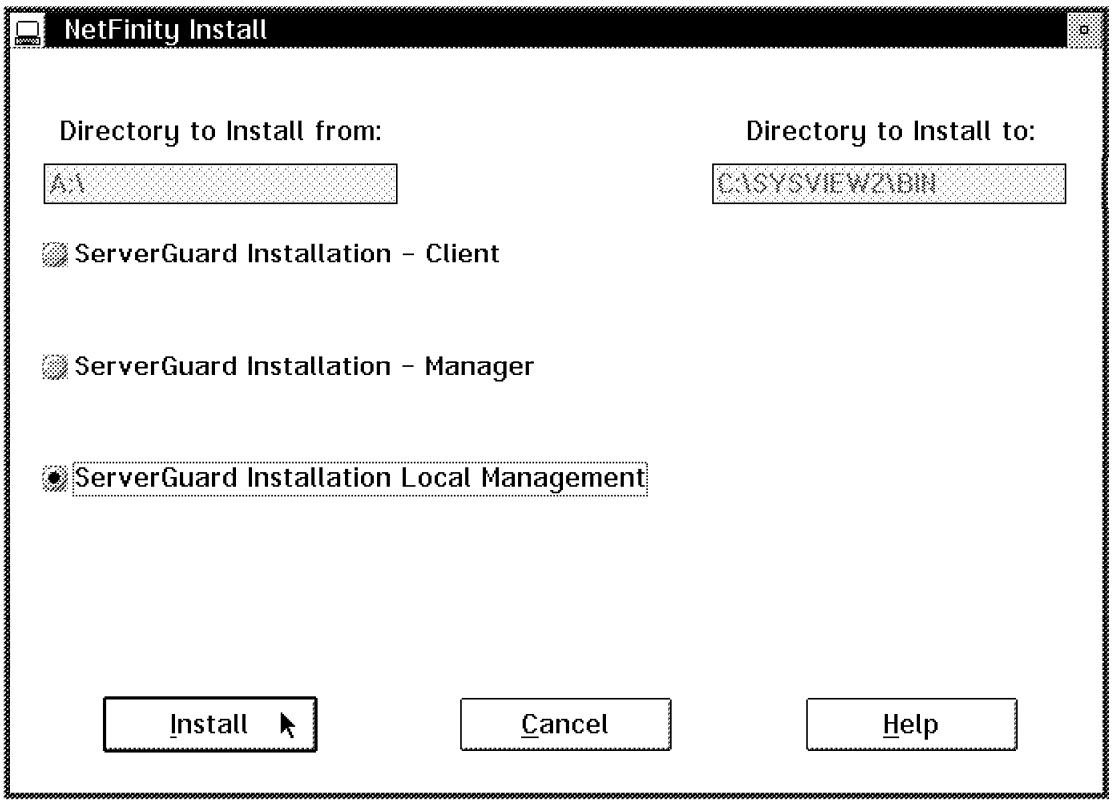


Figure 332. NetFinity Install (Part 2)

- Make your choice and click on **Install**.

  The pop-up window NetFinity Install - Installing appears:

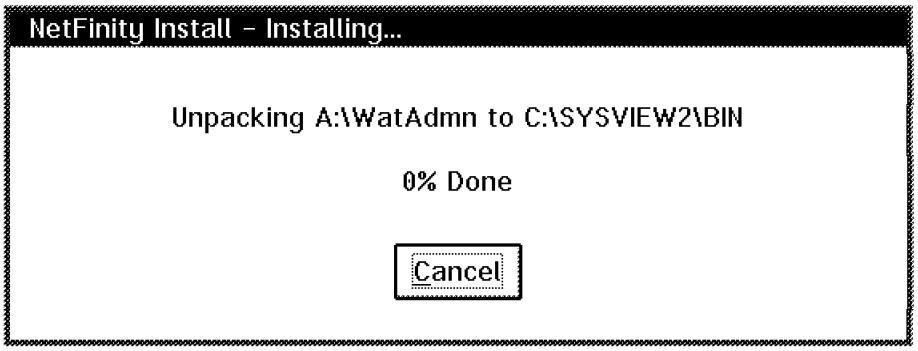


Figure 333. NetFinity Install - Installing

- Click on **Cancel**. The pop-up window Change CONFIG.SYS appears:

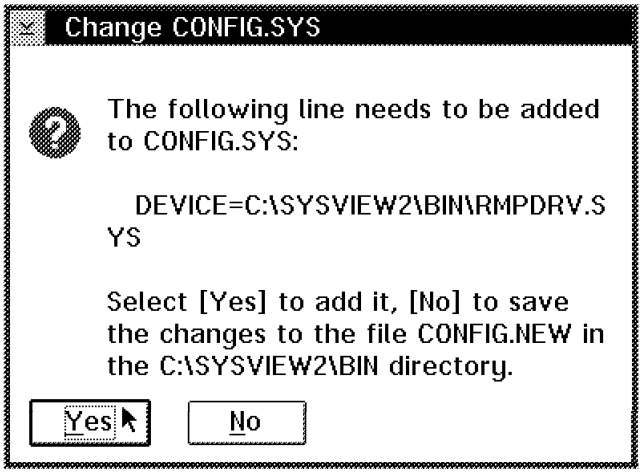


Figure 334. Change CONFIG.SYS

- Click on **Yes** to accept the necessary changes in CONFIG.SYS for the ServerGuard adapter.

  The pop-up window NetFinity Install Complete appears:

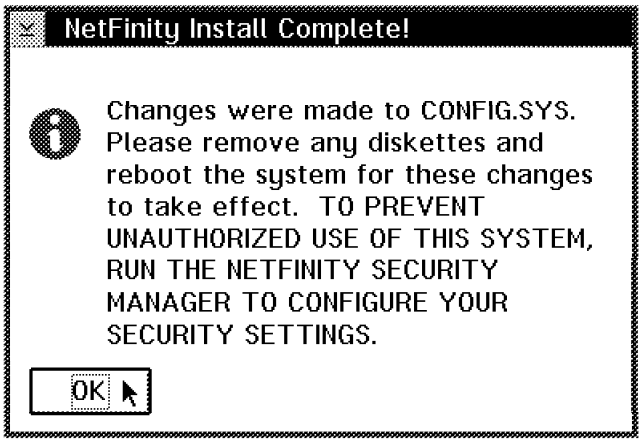


Figure 335. NetFinity Install Complete

- Now you should reboot your machine to let the changes made in CONFIG.SYS become active.

Appendix B. Special Notices

This publication is intended to help automation specialists and systems administrators in a workgroup environment begin to set up some automation using SystemView for OS/2. The information in this publication is not intended as the specification of any programming interfaces that are provided by SystemView for OS/2. See the PUBLICATIONS section of the IBM Programming Announcement for SystemView for OS/2 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (″vendor″) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

ADSTAR	AIX
DB2	DB2/2
FFST/2	IBM

MVS
NetView
OS/400
PS/2
NetFinity
OS/2
Predictive Failure Analysis
SystemView

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

Other trademarks are trademarks of their respective companies.

Appendix C. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

C.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 223.

- *Workgroup Management Using SystemView for OS/2*, SG24-2596
- *LAN Management Processes Using NetFinity*, SG24-4517
- *Software Distribution Using SystemView for OS/2 V1.1*, SG24-4609

A complete list of International Technical Support Organization publications, known as redbooks, with a brief description of each, may be found in:

International Technical Support Organization Bibliography of Redbooks, GG24-3070.

C.2 Other Publications

These publications are also relevant as further information sources.

- *NetView for AIX Administrator's Guide*, SC31-7192

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at URL http://www.redbooks.ibm.com/redbooks.

How IBM Employees Can Get ITSO Redbooks

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet**

  Type GOPHER.WTSCPOK.ITSO.IBM.COM
- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get lists of redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```
- **Redbooks Home Page on the World Wide Web**

  http://w3.itso.ibm.com/redbooks/redbooks.html
- **IBM Direct Publications Catalog on the World Wide Web**

  http://www.elink.ibmlink.ibm.com/pbl/pbl

  IBM employees may obtain LIST3820s of redbooks from this page.
- **ITSO4USA category on INEWS**
- **Online** — send orders to:

  USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

  See explanation under “How Customers Can Get ITSO Redbooks” on page 224.

How Customers Can Get ITSO Redbooks

- **Online Orders** (Do not send credit card information over the Internet)

  IBMMAIL — send orders to:

In United States:	usib6fpl at ibmmail
In Canada:	caibmbkz at ibmmail
Outside North America:	bookshop at dkibmbsh at ibmmail

  Internet — send orders to:

In United States:	usib6fpl@ibmmail.com
In Canada:	lmannix@vnet.ibm.com
Outside North America:	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications	IBM Publications	IBM Direct Services
Publications Customer Support	144-4th Avenue, S.W.	Sortemosevej 21
P.O. Box 29554	Calgary, Alberta T2P 3N5 Canada	DK-3450 Allerød Denmark
Raleigh, NC 27626-0570 USA		

- **Fax** — send orders to:

United States (toll free)	1-800-445-9269
Canada (toll free)	1-800-267-4455
Outside North America (long distance charge)	(+45) 48 14 2207

- **1-800-IBM-4FAX (United States)** or **(+1) 415 855 43 29 (Outside USA)**

  Ask for:
  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services**

  Send note to softwareshop@vnet.ibm.com

- **Redbooks Home Page on the World Wide Web**

  http://www.redbooks.ibm.com/redbooks

- **IBM Direct Publications Catalog on the World Wide Web**

  http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank).

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

- **Please put me on the mailing list for updated versions of the IBM Redbook Catalog.**

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

- Invoice to customer number _____
- Credit card number _____

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

DO NOT SEND CREDIT CARD INFORMATION OVER THE INTERNET.

Index

Printed in U.S.A.